



BladeCenter T 管理模块

用户指南



eserver

BladeCenter T 管理模块

用户指南

注：在使用本资料及其支持的产品之前，请阅读第 67 页的附录 B，『声明』中的一般信息。对本手册所包含的内容，IBM 公司拥有最终解释权。如有变更，恕不另行通知。

第一版（**2004** 年 **5** 月）

目录

安全 v

第 1 章 BladeCenter T 管理模块介绍 1
相关文档 1
本文档中使用的注意事项和声明 2
控件和指示灯 3
  管理模块控件和指示灯 3
  KVM（键盘、视频、鼠标）模块指示灯和输入／输出接口 4
  LAN 模块指示灯和输入／输出接口 6

第 2 章 配置管理模块和 BladeCenter T 单元 9
安装远程连接 11
  以太网端口连线 11
  配置管理模块进行远程访问 13

第 3 章 使用管理模块 Web 界面 15
用户权限 15
启动管理模块 Web 界面 16
管理模块 Web 界面选项 18
  监视器 18
    系统状态 18
    事件日志 21
    指示灯 21
    硬件 VPD 22
    固件 VPD 23
  刀片任务 23
    电源／重新启动 23
    随需应变 24
    远程控制 25
    固件更新 27
    配置 28
    Serial Over LAN 29
  I/O 模块任务 29
    电源／重新启动 30
    管理 30
    固件更新 31
  MM 控制 31
    常规设置 32
    登录概要文件 32
    警报 34
    端口指定 34
    网络接口 35
    网络协议 37
    安全性 38
    配置文件 39
    固件更新 39
    恢复缺省配置 39
    重新启动 MM 40
网络和安全性配置 40

配置 SNMP . . . 40
配置 SMTP . . . 42
配置 LDAP . . . 42
设置客户机以使用 LDAP 服务器 . . . 43
配置 LDAP 客户机认证 . . . 44
配置 LDAP 搜索属性. . . 45
安全 Web 服务器和安全 LDAP . . . 47
配置安全性 . . . 48
SSL 证书概述 . . . 48
SSL 服务器证书管理 . . . 49
为安全 Web 服务器启用 SSL. . . 55
SSL 客户机证书管理 . . . 55
SSL 客户机受信任的证书管理. . . 55
为 LDAP 客户机启用 SSL . . . 57
配置 Secure Shell 服务器 . . . 57
生成 Secure Shell 服务器密钥 . . . 57
启用 Secure Shell 服务器 . . . 58
使用 Secure Shell 客户机 . . . 59
配置 Wake on LAN . . . 59
验证 Wake on LAN 配置 . . . 59
特定于 Linux 的配置 . . . 59
使用配置文件. . . 60
备份当前的配置 . . . 60
恢复和修改 ASM 配置 . . . 61
使用远程磁盘功能 . . . 61

附录 A. 获取帮助和技术协助. . . . 65
在打电话请求服务之前 . . . 65
使用文档 . . . 65
从万维网获取帮助和信息 . . . 65
软件服务和支持 . . . 66
硬件服务和支持 . . . 66

附录 B. 声明 . . . 67
版本声明 . . . 67
商标 . . . 67
重要注意事项. . . 68
产品回收和处理 . . . 69
电池回收计划. . . 69
电子辐射声明. . . 69
联邦通信委员会（FCC）声明 . . . 69
加拿大工业部 A 类辐射一致性声明 . . . 70
澳大利亚和新西兰 A 类声明 . . . 70
英国远程通信安全要求 . . . 70
欧盟 EMC 指令一致性声明 . . . 70
台湾语 A 类警告声明 . . . 71
中文 A 类警告声明 . . . 71
日本干扰自愿控制委员会（VCCI）声明 . . . 71

索引 . . . 73

安全

Before installing this product, read the Safety Information.

قبل تركيب هذا المنتج، يجب قراءة الملاحظات الآمنية

Antes de instalar este produto, leia as Informações de Segurança.

在安装本产品之前，请仔细阅读 Safety Information
（安全信息）。

安裝本產品之前，請先閱讀「安全資訊」。

Prije instalacije ovog produkta obavezno pročitajte Sigurnosne Upute.

Před instalací tohoto produktu ˇsiˇ ̌precťetě prírucků bezpecnostních instrukcí.

Læs sikkerhedsforskrifterne, før du installerer dette produkt.

Lees voordat u dit product installeert eerst de veiligheidsvoorschriften.

Ennen kuin asennat tämän tuotteen, lue turvaohjeet kohdasta Safety Information.

Avant d’installer ce produit, lisez les consignes de sécurité.

Vor der Installation dieses Produkts die Sicherheitshinweise lesen.

Πριν εγκαταστήσετε το προϊόν αυτό, διαβάστε τις πληροφορίες ασφάλειας
(safety information).

לפני שתתקינו מוצר זה, קראו את הוראות הבטיחות.

A termék telepítése előtt olvassa el a Biztonsági előírásokat!

Prima di installare questo prodotto, leggere le Informazioni sulla Sicurezza.

製品の設置の前に、安全情報をお読みください。

본 제품을 설치하기 전에 안전 정보를 읽으십시오.

Пред да се инсталира овој продукт, прочитајте информацијата за безбедност.

Les sikkerhetsinformasjonen (Safety Information) før du installerer dette produktet.

Przed zainstalowaniem tego produktu, należy zapoznać się
z książką "Informacje dotyczące bezpieczeństwa" (Safety Information).

Antes de instalar este produto, leia as Informações sobre Segurança.

Перед установкой продукта прочтите инструкции по технике безопасности.

Pred inštaláciou tohto zariadenia si pečítaje Bezpečnostné predpisy.

Pred namestitvijo tega proizvoda preberite Varnostne informacije.

Antes de instalar este producto, lea la información de seguridad.

Läs säkerhetsinformationen innan du installerar den här produkten.

声明 **1**：



危险

电源、电话和通信电缆中的电流是有危险的。

为避免电击危险：

- 请勿在雷电期间连接或断开本产品的任何电缆的连接，或者进行本产品的安装、维护或重新配置。
- 请将所有电源线连接到已正确连线并且接地的电源插座。
- 将任何要连接到本产品的设备连接到正确连线的插座。
- 如有可能，请仅使用一只手连接或断开信号电缆的连接。
- 请勿在有火、水、结构损坏迹象的情况下开启任何设备。
- 除非在安装和配置过程中另有说明，否则请在打开设备外盖之前断开连接的电源线、远程通信系统、网络和调制解调器。
- 在安装、移动或打开本产品或所连接设备的外盖时，请按下表所述方法连接和断开电缆连接。

要连接：	要断开连接：
1. 关闭所有设备。	1. 关闭所有设备。
2. 首先，将所有电缆连接到设备。	2. 首先，从插座上拔下电源线。
3. 将信号电缆连接到接口。	3. 从接口上拔下信号电缆。
4. 将电源线连接到插座。	4. 从设备上拔下所有电缆。
5. 开启设备。	

声明 **8**：



注意：
请勿卸下电源外盖或贴有以下标签的任何部件的外盖。



贴有此标签的任何组件内部都有危险的电压、电流和能量级别。这些组件内部没有可维修的部件。如怀疑这些部件中的某一个有问题，请联系技术服务人员。

警告：操作本产品上的电源线或与随本产品一起销售的附件相关联的电源线将使您易受铅的伤害，（一种加利福尼亚州已知的导致癌症、生殖缺陷或其它再生性伤害的化学物质）。*请在操作后洗手。*

ADVERTENCIA: El contacto con el cable de este producto o con cables de accesorios que se venden junto con este producto, pueden exponerle al plomo, un elemento químico que en el estado de California de los Estados Unidos está considerado como un causante de cancer y de defectos congénitos, además de otros riesgos reproductivos. ***Lávese las manos después de usar el producto.***

第 1 章 BladeCenter T 管理模块介绍

本《*管理模块用户指南*》包含有关配置管理模块以及管理 IBM® *e*server BladeCenter™ T 单元中安装的组件的信息。

BladeCenter T 单元在管理模块托架 1 中随附一个热交换管理模块。您可以在管理模块托架 2 中安装一个管理模块。在同一时刻这些管理模块中只能有一个活动的模块作为主要管理模块；如果安装了第二个管理模块，它将提供冗余功能。辅助管理模块将保持不活动状态直至将它转换为主要管理模块。

当 BladeCenter T 单元中安装了两个管理模块时，它们必须始终保持支持冗余管理模块功能的相同固件级别。这将有助于确保从活动管理模块将控制平滑交接给冗余管理模块。位于 http://www.ibm.com/pc/support/ 的 IBM Support Web 站点提供最近级别的管理模块固件。

管理模块充当 BladeCenter T 单元中安装的所有刀片服务器的服务处理器和键盘／视频／鼠标（KVM）多路复用器。它控制供本地控制台使用的键盘、鼠标和视频 KVM 模块外部连接。管理模块还控制三个 LAN 模块外部连接：两个用于 10/100 Mbps 以太网远程管理连接的 RJ-45 接口和一个可用于监控 BladeCenter T 状态的警报接口。

管理模块中的服务处理器与每台刀片服务器中的服务处理器进行通信以支持相应功能，例如：刀片服务器供电请求、错误和事件报告、KVM 请求以及使用 BladeCenter T 共享介质托盘（CD-ROM 驱动器和 USB 端口）的请求。

您使用管理模块来配置 BladeCenter T 组件，设置诸如 IP 地址等信息。管理模块与 BladeCenter T 单元中的所有组件进行通信，检测它们是否存在、报告其状态并在需要时发送错误情况的警报。

相关文档

除了本《*用户指南*》外，BladeCenter T 管理模块随附的 IBM *BladeCenter T 文档* CD 以 PDF 格式提供以下文档。

- 《*安全信息*》

  本文档包含翻译过的警告和危险声明。出现在该文档中的每条警告和危险声明都有一个编号，您可以使用此编号在《*安全信息*》文档中找到与您的语言对应的声明。

- *《BladeCenter T 管理模块安装指南》*

  本文档包含在 BladeCenter T 单元中安装 IBM BladeCenter T 管理模块选件和创建初始配置的说明。
- *《BladeCenter T HS20 8832 型硬件维护手册和故障诊断指南》*

  本文档包含帮助您自行解决 BladeCenter T HS20 问题的信息以及供技术服务人员使用的信息。
- *《BladeCenter T 8720 和 8730 型安装和用户指南》*

  本文档包含安装和配置 BladeCenter T 单元的说明以及安装某些选件的基本说明。它还包含有关 BladeCenter T 单元的一般信息。
- *《BladeCenter T 8720 和 8730 型硬件维护手册和故障诊断指南》*

  本文档包含帮助您自行解决 BladeCenter T 问题的信息以及供技术服务人员使用的信息。
- *《BladeCenter T 8720 和 8730 型机架安装说明》*

  本文档包含在机架中安装 BladeCenter T 单元的说明。
- *《IBM eServer BladeCenter Serial over LAN 设置指南》*

  本文档说明了如何更新和配置 BladeCenter 组件以用于 Serial over LAN（SOL）操作。SOL 连接提供了对每台刀片服务器上命令行控制台命令提示符的访问，这样就可以从远程位置对刀片服务器进行管理。

IBM *BladeCenter T 文档* CD 中可能还包含其它文档。

您的刀片服务器可能具有刀片服务器随附的文档中未描述的功能。此文档可能不定期地更新以包含有关这些功能的信息，或者可能有技术更新来提供服务器文档中没有包含的其它信息。这些更新可以从 IBM Web 站点获取。完成以下步骤以检查更新的文档和技术更新：

1. 转至 http://www.ibm.com/pc/support/。
2. 在 **Learn** 部分，单击 **Online publications**。
3. 在 " Online publications " 页面的 **Brand** 字段中，选择 **Servers**。
4. 在 **Family** 字段中，选择 **BladeCenter T**。
5. 单击 **Continue**。

本文档中使用的注意事项和声明

本文档中出现的警告和危险声明也可以在多语言版本的*《安全信息》*文档中找到，该文档在 IBM *BladeCenter T 文档* CD 中。每条声明都进行了编号以便于参考*《安全信息》*文档中的相应声明。

此文档中使用了以下注意事项和声明：

- 注：这些注意事项提供重要的提示、指导或建议。
- 要点：这些注意事项提供可能帮助您避免出现不便或问题的信息或建议。
- 注意：这些注意事项指出对程序、设备或数据可能造成的损坏。该注意事项就位于可能会发生损坏的说明或情况之前。

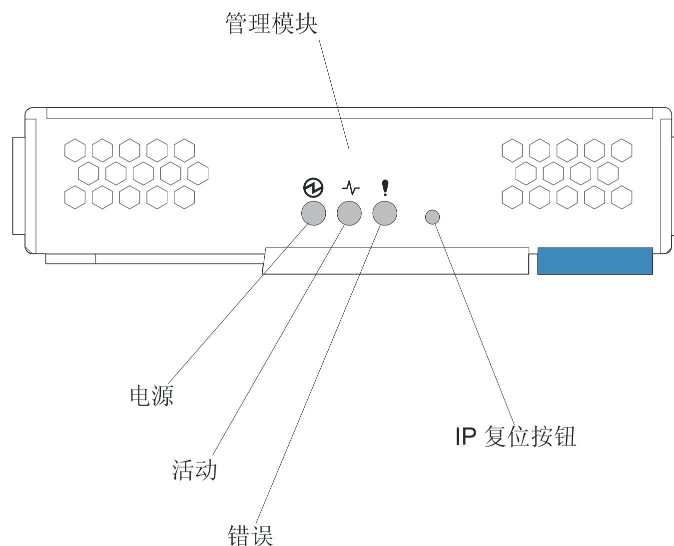
- 警告：这些声明指出对您来说可能具有潜在危险的情况。警告声明就位于具有潜在危险的过程步骤或情况的描述之前。
- 危险：这些声明指出对您来说可能具有潜在致命或极端危险的情况。危险声明就位于具有潜在致命或极端危险的过程步骤或情况的描述之前。

控件和指示灯

本节描述了 BladeCenter T 管理模块、KVM 模块和 LAN 模块上的指示灯和控件。本节还将帮助您识别 KVM 和 LAN 模块上的外部端口。

管理模块控件和指示灯

这些管理模块控件和指示灯提供了有关管理模块和远程管理连接的状态信息。有关其它信息，请参阅 IBM *BladeCenter T 文档* CD 中的《*硬件维护手册和故障诊断指南*》。



管理模块指示灯：这些指示灯提供了有关管理模块和远程管理连接的状态信息。

- 电源：如果这个绿色的指示灯亮着，它表明管理模块已接通电源。
- 活动： 如果这个绿色的指示灯亮着，它表明管理模块正在控制 BladeCenter T 单元。在同一时刻只有一个管理模块控制 BladeCenter T 单元。如果 BladeCenter T 单元中安装了两个管理模块，在同一时刻只有一个指示灯是亮着的。
- 错误： 如果这个淡黄色的指示灯亮着，它表明在管理模块的某个位置检测到错误。如果这个指示灯亮着，每个 BladeCenter T 系统状态面板上的系统错误指示灯（严重、主要或次要）也会亮着。

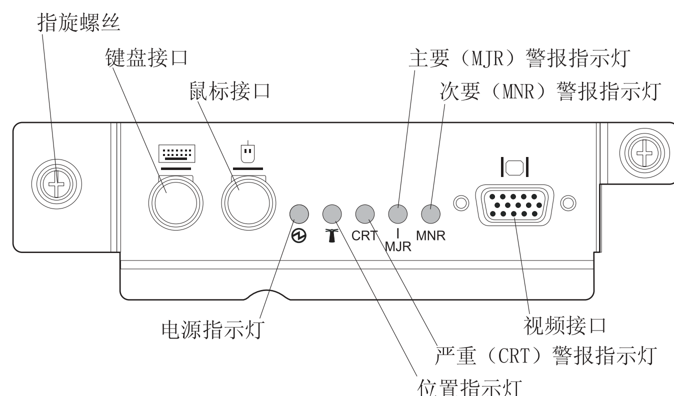
管理模块 **IP** 复位按钮：*请勿*按下这个按钮，除非您要擦除为管理模块配置的 IP 地址并断开与远程管理站、交换机模块和刀片服务器的连接。如果按下这个按钮，您必须对管理模块的设置进行重新配置（请参阅从第 9 页的第 2 章，『配置管理模块和 BladeCenter T 单元』开始的信息以获取相关说明）。

按下这个凹陷式按钮将管理模块网络接口（以太网 1、以太网 2、网关地址等）的 IP 配置重置为出厂缺省值，然后重新启动管理模块。

用一根拉直的回形针即可按下这个按钮。

KVM（键盘、视频、鼠标）模块指示灯和输入／输出接口

KVM 模块是一种安装在 BladeCenter T 单元背面的热交换模块并以外加的指旋螺丝固定到位。这个模块包括两个 PS/2® 接口（供键盘和鼠标使用）、一个系统状态面板和一个 HD-15 视频接口。



系统状态指示灯： 这些指示灯提供 BladeCenter T 单元的状态信息。

- 电源：如果这个绿色的指示灯持续发亮，它表明 BladeCenter T 单元已接通电源。切断电源时，这个指示灯将熄灭。

  警告： 如果电源指示灯不亮，并不表示 BladeCenter T 单元没有接通电源。此指示灯可能已烧毁。要切断 BladeCenter T 单元的所有电源，必须拔下所有电源模块的电源线。
- 位置： 这个蓝色指示灯用于识别系统。系统管理员或服务人员利用这个指示灯来找到要维护或维修的特定 BladeCenter T 单元。您可以通过 Web 界面或远程管理控制台关闭位置指示灯。

警报指示灯：这些指示灯提供 BladeCenter T 单元的警报通知。

- **CRT**（严重警报，淡黄色（缺省颜色）或红色）：如果这个指示灯持续发亮，它表明出现严重系统故障。系统将淡黄色作为缺省颜色。有关设置这个指示灯颜色的信息，请参阅第 21 页的『指示灯』。

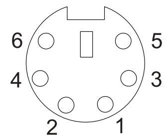
  严重系统故障是不可恢复的错误或事件。在这种情况下，系统将无法继续运行。示例为，丢失大段内存导致系统无法运行。
- **MJR**（主要警报，淡黄色（缺省颜色）或红色）：如果这个指示灯持续发亮，它表明出现主要系统故障。系统将淡黄色作为缺省颜色。有关设置这个指示灯颜色的信息，请参阅第 21 页的『指示灯』。

  主要系统故障是对系统运行造成可以察觉到的影响的错误或事件。在这种情况下，系统可以继续运行，但性能受到一定影响。示例为，丢失两个镜像磁盘中的一个。
- **MNR**（次要警报，淡黄色）：如果这个指示灯持续发亮，它表明出现次要系统故障。次要系统故障是对系统运行影响很小的错误或事件。示例为，可纠正的 ECC 错误。

接口：KVM 模块具有以下 I/O 接口：

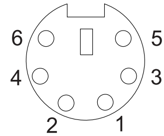
- 键盘接口：BladeCenter T KVM 模块包括一个 PS/2 样式键盘接口。

使用这个接口将 PS/2 键盘连接到 BladeCenter T 单元。



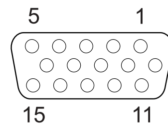
- 鼠标接口：BladeCenter T KVM 模块包括一个 PS/2 样式鼠标接口。

  使用这个接口将 PS/2 鼠标连接到 BladeCenter T 单元。



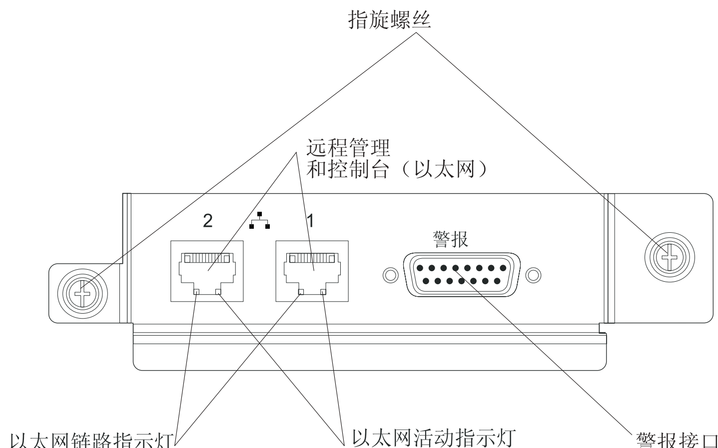
- 视频接口：BladeCenter T KVM 模块包括一个标准视频接口。每台刀片服务器上的集成视频控制器与 SVGA 和 VGA 兼容并可以通过这个视频端口进行通信。

  使用这个接口将视频监视器连接到 BladeCenter T 单元。



LAN 模块指示灯和输入／输出接口

LAN 模块是一种安装在 BladeCenter T 单元背面的热交换模块并以外加的指旋螺丝固定到位。LAN 模块为 BladeCenter T 单元的两个局域网（以太网）连接提供电力和机械接口，它们由各个管理模块和 telco 外部警报驱动。这个模块包括两个带有指示灯的 RJ-45 接口和一个 DSUB 15P telco 警报接口。



LAN 模块指示灯：这些指示灯提供了有关 LAN 连接的状态信息：

- 以太网链路： 如果这个绿色的指示灯亮着，表明存在由这个端口到网络的活动连接。
- 以太网活动：如果这个绿色的指示灯在闪烁，它表明在网络链路上存在通过这个端口的活动。

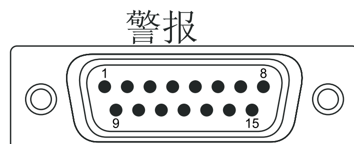
LAN 模块接口：

- 远程管理和控制台（以太网）接口： LAN 模块提供两个以太网 RJ-45 接口。

  BladeCenter T LAN 模块包括两个由各个管理模块驱动的 10/100 Mb 以太网接口，它们提供与网络中网络管理站的远程连接。

  将这些端口用于远程管理和远程控制台。

  网络管理站通过这些接口可以访问在管理模块中正在运行的控制功能、每台刀片服务器上或每个交换机模块中的服务处理器。但是，它不能使用这些端口与刀片服务器中正在运行的应用程序通信。网络管理站必须指引这些通信通过连接到 BladeCenter T 单元中 I/O 模块的外部端口的网络。
- 警报接口： LAN 模块提供一个用于严重、主要和次要 telco 警报的 telco DB15 警报接口（插入式）。每个警报有一个中继设备，它使得多个系统警报指示灯可以串在一起。第 7 页的表 1 列出 telco 警报接口的引脚图。



注：服务处理器、管理模块或系统管理功能必须监控警报复位输入以保持您为单元设置的故障条件。警报复位输入可以是超出标准逻辑级别的电压，在这样情况下您必须在电力方面或光学方面将它们从监控逻辑中隔离出来。

表 1. telco 警报接口引脚图

引脚 #	描述	I/O	引脚 #	描述	I/O
1	次要警报复位 +	I	9	次要警报正常关闭	O
2	次要警报复位 -	I	10	次要警报公共	O
3	主要警报复位 +	I	11	主要警报正常打开	O
4	主要警报复位 -	I	12	主要警报正常关闭	O
5	严重警报正常打开	O	13	主要警报公共	O
6	严重警报正常关闭	O	14	保留	
7	严重警报公共	O	15	保留	
8	次要警报正常打开	O			

警报接口的电子规格如下：

– 输出
  - 电压范围：0 V 直流电至 -100 V 直流电（100 V 直流电时最大电流为 0.3 A）
  - 电流范围：0 A 至 1 A（1 A 时最大电压为 30 V 直流电）
  - 最糟 VA：-30 V 直流电时 1 A（最大 30 VA）不确定

– 输入
  - 电压范围：0 V 直流电至 -100 V 直流电（包括瞬态）
  - 差分输入电压：3 V 直流电至 72 V 直流电

– 复位输入激活

  脉冲宽度：200 ms（最小值）至 300 ms

第 2 章 配置管理模块和 BladeCenter T 单元

要点：您只需配置主要（活动）管理模块。辅助管理模块将根据需要自动从主要管理模块接收配置和状态信息。本章中的配置信息适用于主要管理模块，它可能是 BladeCenter T 单元中安装的唯一管理模块。

BladeCenter T 单元将自动检测安装的模块和刀片服务器并存储重要产品数据（VPD）。当启动 BladeCenter T 单元时，管理模块将自动配置管理模块上的远程管理端口（此端口通过 BladeCenter T 单元背面的 LAN 模块访问），以便您可以配置和管理 BladeCenter T 单元和刀片服务器。您可以使用基于 Web 的用户界面通过管理模块对 BladeCenter T 单元进行远程配置和管理。

注：有两种配置交换机模块的方法：通过管理模块 Web 界面或通过使用 Telnet 界面或 Web 浏览器通过管理模块启用的外部交换机模块端口。有关更多信息，请参阅交换机模块随附的文档。

要使活动的管理模块能与 BladeCenter T 单元中的 I/O 模块进行通信，您必须为以下内部和外部端口配置 IP 地址：

- 管理模块上的外部以太网（远程管理）端口，通过 BladeCenter T 单元背面的 LAN 模块访问它（有关信息，请参阅第 35 页开始的信息）。初始管理模块自动配置使得网络管理站可以连接到管理模块完整地配置端口并对 BladeCenter T 单元的其余部分进行配置。
- 管理模块上的内部以太网端口，它用于与 I/O 模块进行通信（有关信息，请参阅第 35 页开始的信息）。
- 每个交换机模块上的管理端口提供与管理模块的通信。通过配置交换机模块的 IP 地址来配置这一端口（有关信息，请参阅第 30 页开始的信息）。

  注：某些类型的 I/O 模块（如 pass-thru 模块）没有管理端口。

请参阅 I/O 模块随附的文档以确定还必须在 I/O 模块中进行哪些配置。

要与刀片服务器进行通信以实现诸如通过网络来部署操作系统或应用程序等功能，您至少还必须在 I/O 模块托架 1 或 2 中的以太网交换机模块上配置一个外部（频带内）端口。有关配置以太网 I/O 模块上的外部端口的一般信息，请参阅您的 BladeCenter T 单元的《*安装和用户指南*》。

管理模块支持以下用于远程访问的 Web 浏览器。您使用的 Web 浏览器必须支持 Java™、JavaScript™ 1.2 或后续版本并安装 Java 虚拟机（JVM）1.4.1 或后续版本的插件。Java Web 站点中可以找到 JVM 插件，它位于 http://www.java.com/。

- Microsoft® Internet Explorer 5.5（已安装最新的 Service Pack）或后续版本
- Netscape Navigator 4.72 或后续版本（不支持 V6）
- Mozilla V1.3 或后续版本

为获得 Web 浏览器的最佳使用效果，请将监视器设置为 256 色。仅使用下表中给出的视频分辨率和刷新率。这些是唯一支持所有系统配置的视频分辨率和刷新率组合。

分辨率	刷新率
640 x 480	60 赫兹

分辨率	刷新率
640 x 480	72 赫兹
640 x 480	75 赫兹
640 x 480	85 赫兹
800 x 600	60 赫兹
800 x 600	72 赫兹
800 x 600	75 赫兹
800 x 600	85 赫兹
1024 x 768	60 赫兹
1024 x 768	75 赫兹

Web 界面不支持双字节字符集（DBCS）语言。

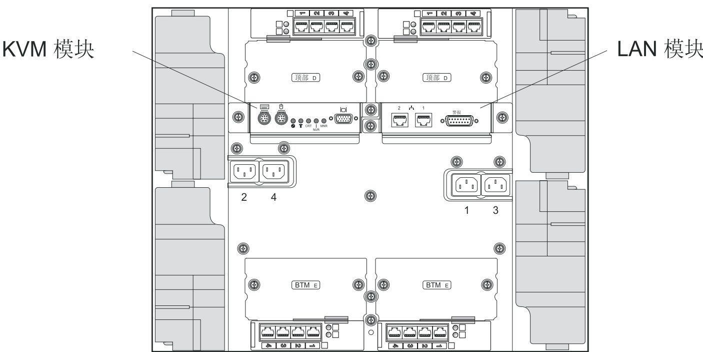
基于 Web 的用户界面与管理和配置程序进行通信，后者是管理模块随附的固件的一部分。您可以使用这个程序执行以下任务：

- 定义登录标识和密码。
- 选择特定事件的警报通知的接收方。
- 监控 BladeCenter T 单元和刀片服务器的状态。
- 控制 BladeCenter T 单元和刀片服务器。
- 访问 I/O 模块对它们进行配置。
- 更改刀片服务器中的启动顺序。
- 设置日期和时间。
- 使用刀片服务器的远程控制台。
- 更改键盘、视频和鼠标的所有权。
- 更改 CD-ROM 驱动器和 USB 端口的所有权。（刀片服务器操作系统将 BladeCenter T 单元中的 CD-ROM 驱动器视作 USB 设备。）
- 激活随需应变的刀片服务器。
- 设置严重（CRT）和主要（MJR）警报指示灯的活动颜色

您还可以使用管理和配置程序查看刀片服务器的部分配置设置。有关更多信息，请参阅第 15 页的第 3 章，『使用管理模块 Web 界面』。

安装远程连接

要配置和管理 BladeCenter T 单元及刀片服务器，您首先必须通过 LAN 模块上的以太网端口安装远程连接。LAN 模块位于 BladeCenter T 单元背面的右上角。

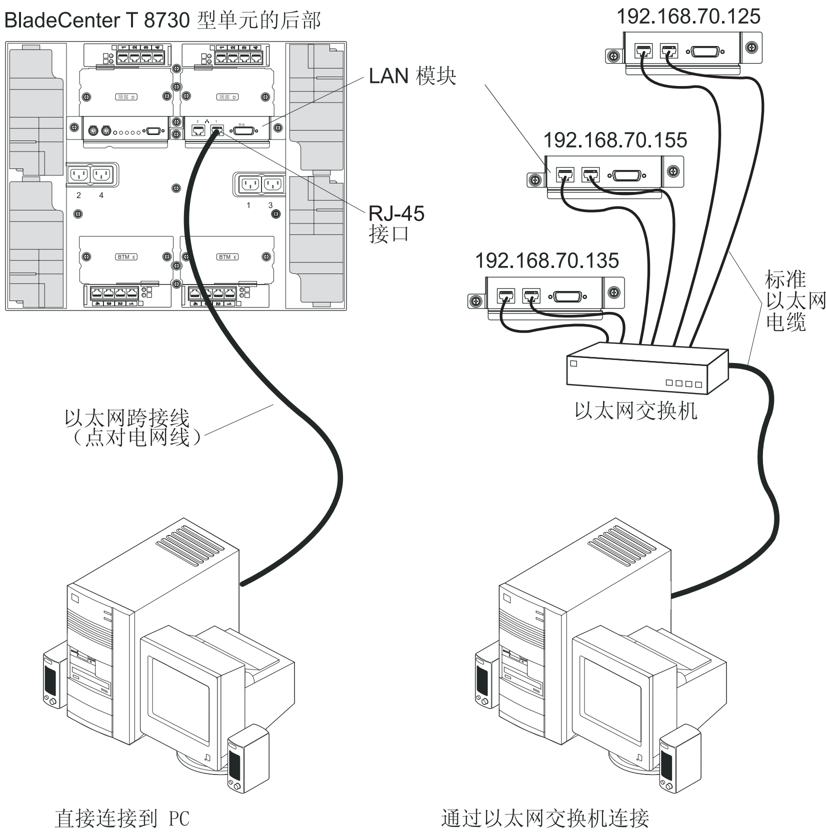


以太网端口连线

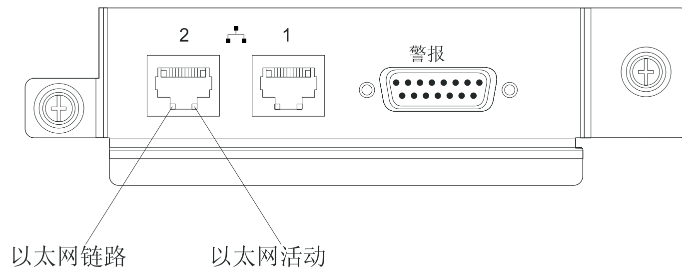
您可以使用跨接线（点对点网线）将个人计算机（PC）直接连接到以太网端口或是通过以太网交换机进行连接。

LAN 模块右侧的以太网端口由管理模块 1 驱动，而 LAN 模块左侧的以太网端口则由管理模块 2 驱动。

完成以下步骤将以太网电缆连接到管理模块。



1. 将 5 类或更高类别的以太网电缆的一端连接到 LAN 模块上的一个以太网接口。将以太网电缆的另一端连接到网络。
2. 检查以太网指示灯以确保网络连接工作正常。下图显示了 LAN 模块上以太网指示灯的位置。



以太网链路指示灯
: 如果这个绿色的指示灯亮着，表明存在由这个端口到网络的活动连接。

以太网活动指示灯
: 如果这个绿色的指示灯在闪烁，它表明在网络链路上存在通过这个端口的活动。

配置管理模块进行远程访问

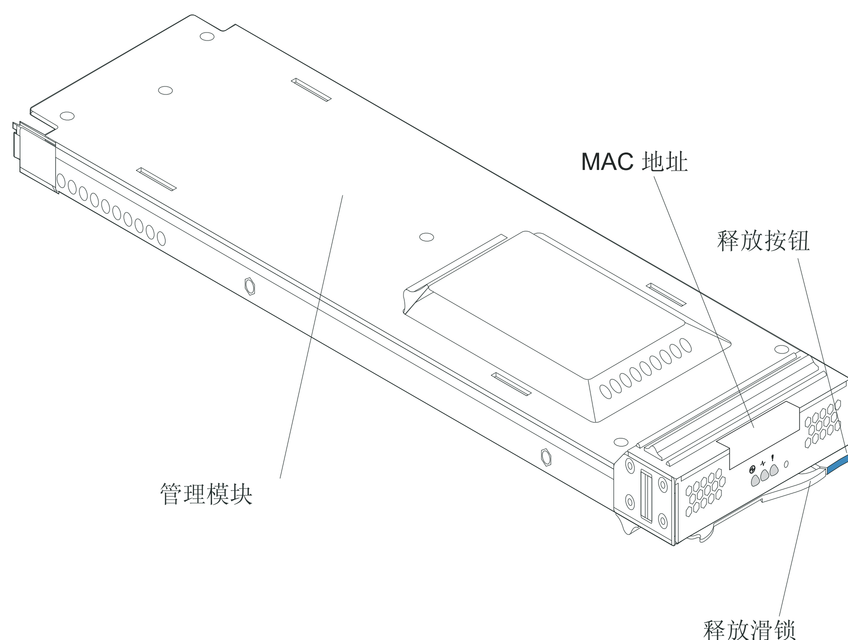
将活动的管理模块连接到网络后，使用以下一种方式配置以太网端口连接：

- 如果您的网络上有一台可访问、已配置的活动动态主机配置协议（DHCP）服务器，将自动设置主机名、IP 地址、网关地址、子网掩码和 DNS 服务器 IP 地址。
- 如果在连接端口后的 2 分钟内，DHCP 服务器仍没有响应，管理模块将使用出厂时定义的静态 IP 地址和缺省子网地址。

这两种操作都能启用活动管理模块上的以太网连接。

确保您的计算机与管理模块在同一子网中；然后使用 Web 浏览器连接到管理模块（有关更多信息，请参阅第 16 页的『启动管理模块 Web 界面』）。在浏览器地址字段中，指定管理模块正在使用的 IP 地址：

- 如果 IP 地址是通过 DHCP 服务器指定的，请从网络管理员那里获取 IP 地址。
- 出厂时定义的静态 IP 地址是 192.168.70.125，缺省的子网地址是 255.255.255.0，缺省的主机名是 MM*xxxxxxxxxxxx*，其中 *xxxxxxxxxxxx* 是内建介质访问控制（MAC）地址。MAC 地址位于管理模块正面指示灯上方的标签上，如下图所示。



注：如果 IP 配置是由 DHCP 服务器指定的，网络管理员可以使用管理模块网络接口的 MAC 地址来确定指定了哪个 IP 地址和主机名。

第 3 章 使用管理模块 Web 界面

本节提供在活动（主要）管理模块中使用管理模块 Web 界面的说明。它包括以下信息：

- 用户可以根据其权限级别访问的管理模块 Web 界面的功能（请参阅『用户权限』）
- 第 16 页的『启动管理模块 Web 界面』
- 管理模块 Web 界面页面的描述（请参阅第 18 页的『管理模块 Web 界面选项』）
- 第 40 页的『网络和安全性配置』
- 第 59 页的『配置 Wake on LAN』
- 管理模块配置的备份和恢复（请参阅第 60 页的『使用配置文件』）

用户权限

只有被授予对那些页面具有必需的相应级别权限的用户才能更改或执行管理模块 Web 界面页面中的某些字段和选项。查看信息不需要任何特殊的命令权限。具有超级用户（Supervisor）命令权限的用户可以在所有页面中更改信息和执行任务。

下表列出了各个管理模块 Web 界面页面以及更改相应页面中的信息所需的权限级别。此表中列出的页面和权限仅适用于更改页面中的信息或执行页面中指定的任务。查看页面中的信息不需要任何特殊的命令权限。表中的每一行表明允许用户更改页面中的信息或执行页面中相应任务的有效用户命令权限。例如，具有“超级用户”权限的用户或具有刀片及 I/O 模块电源／重新启动访问权限的用户可以执行刀片任务 → 电源／重新启动页面中的任务。

表 2. 用户权限关系

页面		更改信息或执行任务所需的权限								
		超级用户	用户帐户管理	刀片服务器远程控制台访问	刀片服务器远程控制台和虚拟介质访问	刀片和 **I/O** 模块电源／重新启动访问	清除事件日志的能力	基本配置（**MM**、**I/O** 模块、刀片）	网络和安全性配置	高级配置（**MM**、**I/O** 模块、刀片）
监视器	系统状态	•	•	•	•	•	•	•	•	•
	事件日志（查看）	•	•	•	•	•	•	•	•	•
	事件日志（清除）	•					•			
	指示灯	•	•	•	•	•	•	•	•	•
	硬件 VPD	•	•	•	•	•	•	•	•	•
	固件 VPD	•	•	•	•	•	•	•	•	•
刀片任务	电源／重新启动	•				•				
	随需应变	•				•				
	远程控制（远程控制台）	•		•	•					
	远程控制（虚拟介质）	•			•					
	固件更新	•								•
	配置	•						•		•
	Serial over LAN	•							•	•
I/O 模块任务	电源／重新启动	•				•				
	管理	•							•	•
	固件更新	•								•
MM 控制	常规设置	•						•		•
	登录概要文件	•	•							•
	警报	•						•		•
	端口指定	•							•	•
	网络接口	•							•	•
	网络协议	•							•	•
	安全性	•							•	•
	配置文件	•								•
	固件更新	•								•
	恢复缺省配置	•								•
	重新启动 MM	•								•

启动管理模块 **Web** 界面

完成以下步骤来启动管理模块 Web 界面：

1. 打开 Web 浏览器。在地址或 URL 字段中，输入为管理模块远程连接定义的 IP 地址或主机名（有关详细信息，请参阅第 13 页的『配置管理模块进行远程访问』）。

   将打开“ 输入网络密码 ”页面。

2. 输入您的用户名和密码。如果这是您第一次登录管理模块，您可以从系统管理员那里获得用户名和密码。事件日志中将记录所有登录尝试操作。

   注：管理模块出厂时定义的初始用户标识和密码如下：

   - 用户标识：USERID（全部为大写字母）
   - 密码：PASSW0RD（注意“ PASSW0RD ”中的零，而不是字母“ O ”）

3. 按照屏幕上的指示信息操作。务必为 Web 会话设置期望的超时值。

将打开 BladeCenter T 管理模块 Web 界面页面。

IBM. BladeCenter T Management Module eserver

Bay 1: SN#01

- Monitors
  - System Status
  - Event Log
  - LEDs
  - Hardware VPD
  - Firmware VPD
- Blade Tasks
  - Power/Restart
  - On Demand
  - Remote Control
  - Firmware Update
  - Configuration
  - Serial Over LAN
- I/O Module Tasks
  - Power/Restart
  - Management
  - Firmware Update
- MM Control
  - General Settings
  - Login Profiles
  - Alerts
  - Port Assignments
  - Network Interfaces
  - Network Protocols
  - Security
  - Configuration File
  - Firmware Update
  - Restore Defaults
  - Restart MM

Log Off

System Status Summary

System is operating normally. All monitored parameters are OK.

The following links can be used to view the status of different components.

Blade Servers
I/O Modules
Management Modules
Power Modules
Blowers

Blade Servers

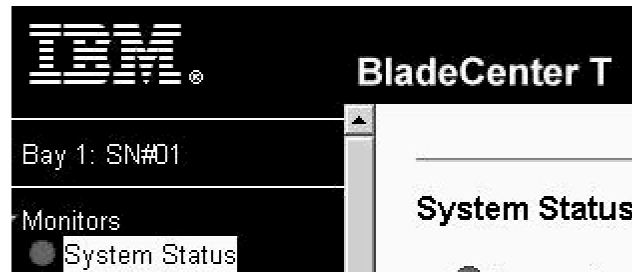
Click the icon in the Status column to view detailed information about each blade server.

Bay	Status	Name	Pwr	Owner**		Network		WOL*	Local Control			BSE*
				KVM	MT*	Onboard	Card		Pwr	KVM	MT*	
1	●	SN#K10V7363140	Off			Eth	--- | ---	On	X	X	X	
2	●	SN#K10V7364105	Off			Eth	--- | ---	On	X	X	X	
3 4	●	Blade 04	Off			Eth	--- | ---	On	X	X	X	
5		*No blade present*										
6	●	SN#K10UJ353166	Off	X	X	Eth	--- | ---	On	X	X	X	
7		*No blade present*										
8		*No blade present*										

* MT = Media Tray (CD/USB) , WOL = Wake on LAN , BEM = Blade Expansion Module ,
BSE = Blade Storage Expansion , BPE = Blade PCI Expansion

** You can change the KVM and Media Tray ownership on the Remote Control panel (under Blade Tasks).

注：管理模块 Web 界面页面的左上角显示了活动（主要）管理模块的位置和标识。在下例中，主要管理模块标识为 SN#01 并安装在管理模块托架 1 中。



管理模块 Web 界面选项

从管理模块 Web 界面中运行管理和配置程序来选择要查看或更改的 BladeCenter T 设置。

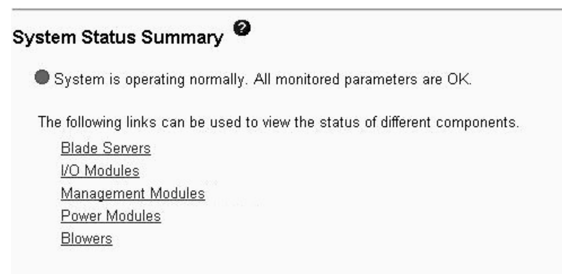
导航窗格（管理模块 Web 界面窗口左侧）包含了用于管理 BladeCenter T 单元和检查组件（模块和刀片服务器）状态的导航链接。以下部分描述了导航窗格中的各个链接。

管理模块 Web 界面提供联机帮助。单击相应部分或选项旁的帮助（？）图标来显示有关此项的更多信息。

监视器

选择监视器部分中的选项来查看 BladeCenter T 单元中各个组件的状态、设置和其它信息。

系统状态



选择系统状态来查看系统的整体状态，一系列需要立即查看的重要事件以及 BladeCenter T 单元中每台刀片服务器及其它组件的整体状态。

Blade Servers

Click the icon in the Status column to view detailed information about each blade server.

Bay	Status	Name	Pwr	Owner**		Network		WOL*	Local Control			BSE*
				KVM	MT*	Onboard	Card		Pwr	KVM	MT*	
1		SN#K10V7363140	Off			Eth	--- | ---	On	X	X	X	
2		SN#K10V7364105	Off			Eth	--- | ---	On	X	X	X	
3		Blade 04	Off			Eth	--- | ---	On	X	X	X	
4												
5		*No blade present*										
6		SN#K10UJ353166	Off	X	X	Eth	--- | ---	On	X	X	X	
7		*No blade present*										
8		*No blade present*										

* MT = Media Tray (CD/USB) , WOL = Wake on LAN , BEM = Blade Expansion Module , BSE = Blade Storage Expansion , BPE = Blade PCI Expansion

** You can change the KVM and Media Tray ownership on the Remote Control panel (under Blade Tasks).

单击刀片服务器时，将显示以下信息：

- 托架 － 刀片服务器占用的编号最小的托架。
- 状态 － 表明刀片服务器状态为良好、警告或故障的图标。有关状态的更多详细信息，请单击此图标。
- 名称 － 刀片服务器的名称。
- 电源 － 刀片服务器的电源状态（开或关）。
- 所有者 － 表明刀片服务器是不是以下 BladeCenter T 资源的当前所有者：
  - **KVM** － 键盘、视频和鼠标
  - **MT** － 包含 CD-ROM 驱动器和 USB 端口的介质托盘
- 网络 － 表明哪些网络接口在刀片服务器（板载）和 I/O 扩展选件（卡）上。例如，板载状态 `Eth` 表明刀片服务器在系统板上集成了以太网控制器，而卡状态 `Fibre` 则表明刀片服务器装有光纤通道 I/O 扩展选件。
- **WOL** － 表明当前是否为刀片服务器启用了 Wake on LAN® 功能。在缺省情况下，将启用刀片服务器 BIOS 中的 Wake on LAN 功能并且无法禁用它。BladeCenter T 管理模块为 Wake on LAN 功能提供了单个控制点，使您能够控制整个 BladeCenter T 单元或是某台刀片服务器的设置。管理模块中进行的 Wake on LAN 设置将覆盖刀片服务器 BIOS 中的设置。有关信息，请参阅第 23 页的『电源／重新启动』。
- 本地控制 － 表明是否启用了以下选项：
  - 本地电源控制
  - 本地键盘、视频和鼠标切换
  - 本地 CD-ROM 驱动器和 USB 端口切换
- **BSE** － 表明 SCSI 扩展单元是否占用刀片托架。

I/O Modules

Bay	Status	Type*	MAC Address	IP Address	Pwr	POST Status
1		Ethernet SM	00:05:5D:89:A3:A0	192.168.70.127	On	POST results available: FF: Module completed POST
2			*No module present*			
3			*No module present*			
4			*No module present*			

* SM = Switch Module, CM = Concentrator Module, PM = Pass-thru Module

单击 **I/O** 模块时，将显示以下信息：

- 托架 — I/O 模块占用的托架的编号。
- 状态 — 表明 I/O 模块状态为良好、警告或故障的图标。
- 类型 — 托架中的 I/O 模块的类型，例如：以太网 I/O 模块、光纤通道 I/O 模块或 pass-thru 模块。
- **MAC** 地址 — I/O 模块的介质访问控制（MAC）地址。

  注：某些类型的 I/O 模块（如 pass-thru 模块）既没有 MAC 地址，也没有 IP 地址。
- **IP** 地址 — I/O 模块的 IP 地址。
- 电源 — I/O 模块的电源状态（开或关）。
- 详细信息 — 有关 I/O 模块状态的文本信息。

Management Modules

Click the icon in the Status column for details about the primary management module.

Bay	Status	IP Address (external n/w interface)	Primary
1	●	192.168.70.125	X
2		*No MM present*	

单击管理模块时，将显示以下信息：

- 托架 — 管理模块占用的托架的编号。
- 状态 — 表明管理模块状态为良好、警告或严重的图标。单击图标以获取状态的更多详细信息，如 BladeCenter T 单元的自测结果、电源电压级别和内部温度。
- **IP** 地址 — 管理模块上的远程管理和控制台连接（外部以太网端口）的 IP 地址。
- 主要 — 表明哪个管理模块是主要管理模块（活动管理模块）。

Power Modules

Bay	Status	Details
1	●	Power module status OK
2	●	Power module status OK
3		*No power module*
4		*No power module*

单击电源模块时，将显示以下信息：

- 托架 — 电源模块占用的托架的编号。
- 状态 — 表明电源模块状态为良好、警告或严重的图标。
- 详细信息 — 有关电源模块状态的文本信息。

Blowers

Bay	Status	Speed (% of max)
1	●	43%
2	●	43%
3	●	43%
4	●	41%

单击送风机时，将显示以下信息：

- 托架 — 送风机模块占用的托架的编号。
- 状态 — 表明送风机模块状态为良好、警告或严重的图标。
- 转速 — 送风机模块的当前转速，以每分钟最大转速（转／分钟）的百分比表示。送风机转速因热量负荷不同而异。脱机条目表明送风机出现故障。

事件日志

Event Log

☑ Monitor log state events

Severity	Source	Date	
E Error W Warning I Info	SERVPROC	02/26/04 02/25/04 02/24/04	Filter Disable Filter

Note: Hold down Ctrl to select more than one option.
Hold down Shift to select a range of options.

Filters: None

Index	Sev	Source	Date/Time	Text
1	I	SERVPROC	02/26/04, 10:14:36	Remote Login Successful. Login ID:"USERID' from WEB browser at IP@=192.168.70.101'
2	I	SERVPROC	02/26/04, 10:14:14	Remote Login Successful. Login ID:"USERID' from WEB browser at IP@=192.168.70.101'
3	I	SERVPROC	02/26/04, 10:13:35	Remote Login Successful. Login ID:"USERID' from WEB browser at IP@=192.168.70.101'
4	I	SERVPROC	02/26/04, 10:13:26	Remote access attempt failed. Invalid userid or password received. Userid is 'USERID' from WEB browser at IP@=192.168.70.101
5	I	SERVPROC	02/26/04, 10:13:20	Remote access attempt failed. Invalid userid or password received. Userid is 'USERID' from WEB browser at IP@=192.168.70.101
6	I	SERVPROC	02/26/04, 09:58:51	Blade Server 6 was installed.
7	I	SERVPROC	02/26/04, 09:58:11	Blade Server 7 was removed.

选择事件日志来查看当前存储在管理模块事件日志中的条目。此日志中包含了刀片服务器检测到的事件条目。日志首先显示最新的条目。所有试图远程访问的相关信息将记录在事件日志中，管理模块将发出相应的警报（如果将它这样配置的话）。

事件日志的最大容量是 750 个条目。当日志达到最大容量的 75% 时，BladeCenter T MNR（次要警报）指示灯将亮起。当日志达到最大容量时，新条目将覆盖最旧的条目并且 BladeCenter T MJR（主要警报）指示灯将亮起。如果您希望由管理模块来监控事件日志的状态，请清除事件日志页面顶部的监控日志状态事件复选框。

您可以对事件日志中的条目进行排序和过滤。有关更多信息，请参阅事件日志帮助。

指示灯

选择指示灯来查看 BladeCenter T 系统状态面板和刀片服务器控制面板指示灯的状态。您还可以使用此选项来打开、关闭或闪烁 BladeCenter T 单元和刀片服务器上的位置指示灯并控制指示灯对警报的响应方式。

将显示以下信息：

- 正面面板和背面面板指示灯 — 控制并显示 BladeCenter T 系统指示灯面板上以下指示灯的状态：
  - 严重警报（CRT 指示灯）
  - 主要警报（MJR 指示灯）
  - 次要警报（MNR 指示灯）
  - 位置

您可以更改位置指示灯的状态并为严重和主要警报指示灯选择活动指示灯颜色（红色或淡黄色）。这一颜色选择适用于 BladeCenter T 单元正面和背面的指示灯以及此页面中显示的指示灯。您还可以指定管理模块是在出现所有类型的警报（严重、主要或次要）时亮起指示灯，还是仅在出现最高级别的警报时亮起指示灯。严重和主要警报指示灯的缺省颜色是淡黄色。管理模块的缺省设置是在出现所有类型的警报（严重、主要或次要）时亮起指示灯。

- 设置警报面板指示灯 — 设置一条描述性的文本消息，它与指定严重性级别的警报相关联。当出现相应严重性级别的警报时，此消息将显示在系统状态页面中。与警报严重性级别相关联的指示灯也可能亮起。
- 刀片服务器指示灯 — 刀片服务器控制面板上以下指示灯的状态。您可以更改信息和位置指示灯的状态。
  - 电源
  - 错误
  - 信息
  - 键盘、视频和监视器选择
  - 介质（CD-ROM 和 USB 端口）选择
  - 位置

硬件 VPD

BladeCenter System VPD

Type / Model	87301XZ
Serial no.	23A0001
UUID	A7FB FB81 DB12 11D6 8D71 C8D6 4BF2 ED0C

Edit BladeCenter System VPD

BladeCenter Hardware VPD

Move your mouse pointer over a module name to see a description for that module in the status bar of your browser.

Bay(s)	Module Name	Manuf. ID	Machine Type/Model	Machine Serial No.	Hardware Revision	Manuf. Date	Part Number	FRU Number	FRU Serial N
Chassis and Media Tray									
	Chassis	IBM	87301XZ	----	2	4603	90P3678	90P3696	347ICHT
1	Media Tray	----	n/a	n/a	0	----	----	----	----
Blade Servers									
3-4	Blade 04	Intel	883931X	23A0119		----		90P0978	
	Daughter Card	Unable to read VPD.							
	Daughter Card	Unable to read VPD.							
5	SN#K10V7363140	SLRM	867841X	KPHT239	8	2303	73P9120	73P9121	K10V73
6	SN#K10UJ353166	SLRM	867841X	KPHT163	8	1803	71P8790	59P6610	K10UJ3
8	SN#K10V7364105	SLRM	867841X	KPHT213	8	2303	73P9120	73P9121	K10V73

选择硬件 **VPD** 来查看 BladeCenter T 单元的硬件重要产品数据（VPD）。启动 BladeCenter T 单元时，管理模块将收集重要产品数据并将它存储在非易失性存储器中。向 BladeCenter T 单元添加组件或从中卸下组件时，管理模块将修改存储的 VPD。您还可以在页面底部查看已安装到 BladeCenter T 单元中或从中卸下的模块的日志。

固件 VPD

Blade Server Firmware VPD

Bay(s)	Name	Firmware Type	Build ID	Released	Revision
3-4	Blade 04	BIOS	SBX44.B05	10/30/2003	0002
		Diagnostics	05AUS		SBY1
		Blade sys. mgmt. proc.	BRMK08A	n/a	8
5	SN#K10V7363140	BIOS	BRE120AUS	03/30/2003	1.02
		Diagnostics	BRYT07AUS	10/30/2002	1.00
		Blade sys. mgmt. proc.	BR8T13A	n/a	13
6	SN#K10UJ353166	BIOS	BRE120AUS	03/30/2003	1.02
		Diagnostics	BRYT07AUS	10/30/2002	1.00
		Blade sys. mgmt. proc.	BR8T13A	n/a	13
8	SN#K10V7364105	BIOS	BRE120AUS	03/30/2003	1.02
		Diagnostics	BRYT07AUS	10/30/2002	1.00
		Blade sys. mgmt. proc.	BR8T13A	n/a	13

I/O Module Firmware VPD

Bay	Type	Firmware Type	Build ID	Released	Revision
There are no I/O modules installed.					

Management Module Firmware VPD

Bay	Name	Firmware Type	Build ID	File Name	Released	Revision
1	SN#01	Main application	BVETJLe	CNETMNUS.PKT	02-25-04	16

选择固件 **VPD** 来查看 BladeCenter T 单元中的所有刀片服务器、I/O 模块和管理模块中的固件重要产品数据（VPD）。固件 VPD 可用于识别固件类型、构件标识、发布日期和修订版编号。管理模块中固件的 VPD 还包含固件组件的文件名。（选择固件 **VPD** 后，最多 30 秒后即可刷新和显示信息。）

刀片任务

选择刀片任务部分中的选项来查看和更改 BladeCenter T 单元中刀片服务器的设置或配置。

电源／重新启动

Blade Power / Restart

Click the checkboxes in the first column to select one or more blade servers; then, click one of the links below the table to perform the desired action.

	Bay	Name	Pwr	Local Pwr Control	Wake on LAN	Console Redirect	SCOD†
	1	SN#K10V7363140	Off	Enabled	On		
	2	SN#K10V7364105	Off	Enabled	On		
	3 4	Blade 04	Off	Enabled	On		
	5	SN#K10WE39F17P	Off	Enabled	On		X
	6	SN#K10UJ353166	Off	Enabled	On		
	7	*No blade present*					
	8	*No blade present*					

† SCOD = Standby Capacity on Demand

Power On Blade
Power Off Blade
Restart Blade
Enable Local Power Control
Disable Local Power Control
Enable Wake on LAN
Disable Wake on LAN
Restart Blade System Mgmt Processor

选择电源／重新启动对 BladeCenter T 单元中的任何刀片服务器执行以下操作。

注：不能在“待机”状态下（以 SCOD 列中的 X 表示）对随需应变的刀片服务器执行这些操作。要激活一台随需应变的刀片服务器，请参阅『随需应变』中的说明。

- 开启或关闭选定的刀片服务器（将电源状态设置为开或关）。
- 启用或禁用本地电源控制。启用本地电源控制时，本地用户可以按下刀片服务器上的电源控制按钮来开启或关闭它。
- 启用或禁用 Wake on LAN 功能。
- 重新启动刀片服务器或刀片服务器中的服务处理器。
- 查看哪些刀片服务器当前处于远程控制台控制之下（以“控制台重定向”列中的 X 表示）。

选择要对它执行操作的刀片服务器；然后单击表下方要执行操作的相应链接。

随需应变

On Demand Blade Activation

Click the checkboxes in the first column to select one or more On Demand blade servers that have a Standby status; then, click the 'Activate Standby Blade Servers' link below to activate the selected blade servers.

Note: You must contact IBM within 14 calendar days after you activate an On Demand blade server. See your Agreement for Standby Capacity on Demand for additional information.
Activating an On Demand blade server restarts the Blade System Management Processor on the blade server. It will take a few minutes for the status of the activated blade server to change from Standby to Active.

Select	Bay	Name	On Demand
	1	SN#K10V7363140	N/A
	2	SN#K10V7364105	N/A
	3 4	Blade 04	N/A
☑	5	SN#K10WE39F17P	Standby
	6	SN#K10UJ353166	N/A
	7	*No blade present*	
	8	*No blade present*	

Activate Standby Blade Servers

选择随需应变来激活一台处于“待机”状态的随需应变的刀片服务器。您必须激活处于“待机”状态的随需应变的刀片服务器才能开启它。激活随需应变的刀片服务器时，其状态将从“待机”变为“活动”，刀片服务器即可投入使用。

在“选择”列中为一台或多台处于“待机”状态的随需应变的刀片服务器选择复选框；然后单击激活待机刀片服务器链接以激活选定的那些刀片服务器。随需应变状态为“不适用”刀片服务器不是随需应变的刀片服务器。

注：在激活随需应变的刀片服务器的 14 天内，您必须与 IBM 联系。有关其它信息，请参阅您的*随需应变待机容量协议*。

远程控制

Remote Control Status

KVM owner: Blade8 - SN#K10V7364105 since 02/23/2004 15:14:53
Media tray owner: Blade8 - SN#K10V7364105 since 02/23/2004 15:15:00
Console redirect: No session in progress.

Refresh

Start Remote Control

To disable the buttons located on the blade servers for KVM and media tray switching, check the boxes below and click "Save". Click "Start Remote Control" to control a blade server remotely. A new window will appear that provides access to the Remote Console and Remote Disk functionality. On this window, you will have full keyboard and mouse control of the blade server which currently owns the KVM. You will also be able to change KVM and media tray ownership.

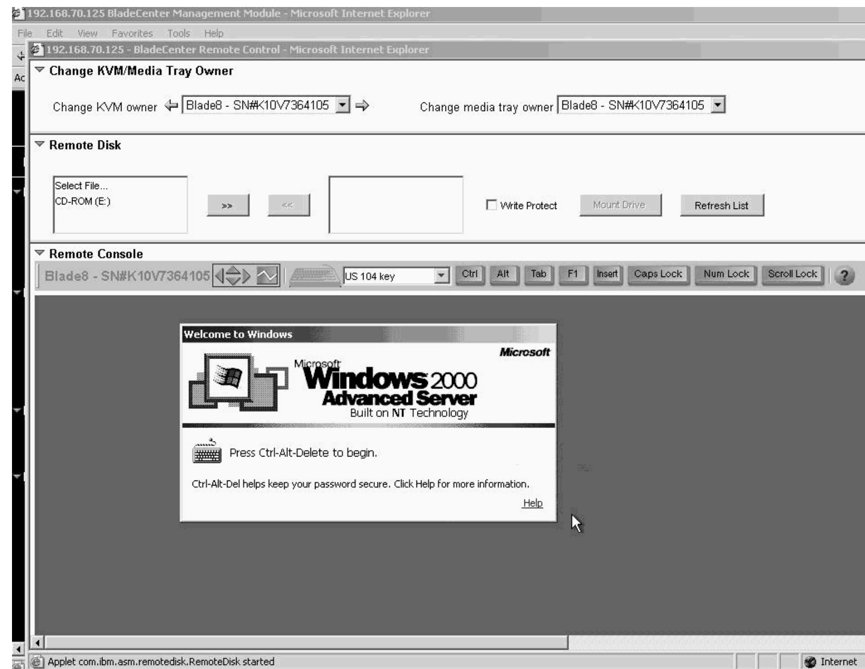
Note: An Internet connection is required to download the Java Runtime Environment (JRE) if the Java 1.4 Plug-in is not already installed.

☐ Disable local KVM switching
☐ Disable local media tray switching

Save Start Remote Control

选择“远程控制”选项来执行以下任务：

- 查看和更改键盘、监视器和鼠标（KVM）以及 CD-ROM 驱动器和 USB 端口（介质托盘）的当前所有者。
- 查看任何当前活动的远程控制会话（用户标识、客户机 IP 地址、启动时间）的详细信息。
- 禁用所有刀片服务器的 KVM 和介质托盘的本地切换直至再次明确启用它们。这可以防止在您执行远程控制任务时，本地用户将控制台显示切换到不同的刀片服务器。
- 将刀片服务器控制台重定向到远程控制台。



在远程控制台上，您可以执行以下任务：

- 将 KVM 和介质托盘的所有者更改为您要查看的刀片服务器。
- 选择并访问介质托盘中的磁盘驱动器。
- 将作为远程控制台的计算机上的一个磁盘驱动器或磁盘映像安装到刀片服务器上。安装的磁盘驱动器或磁盘映像将显示为连接到刀片服务器的 USB 设备。有关信息和说明，请参阅第 61 页的『使用远程磁盘功能』。
- 访问任何可用网络位置的文件。
- 查看当前的刀片服务器显示。
- 象在本地控制台上一样控制刀片服务器，包括重新启动刀片服务器和查看 POST 进程（完全控制键盘和鼠标）。

远程控制台键盘支持包括所有键。对于具有刀片服务器特殊含义的键将提供相应的图标。例如，为了将 Ctrl+Alt+Del 发送到刀片服务器，您必须单击 **Ctrl** 图标，然后按下键盘上的 Alt 和 Del 键。

在同一时刻只允许一个远程控制会话。如果已有一个远程控制会话处于活动状态，您可以终止当前会话并启动一个新会话。

远程控制会话的超时值与您登录时为管理模块 Web 界面会话设置的超时值相同。

当您将刀片服务器 Linux X Window System 会话控制台重定向到远程控制台时，远程控制台 applet 精确跟踪鼠标光标位置的能力取决于 X Window System 的配置。完成以下过程对 X Window System 进行配置以实现精确的鼠标跟踪。通过远程控制台或在连接到 BladeCenter T 单元的键盘上输入命令。请注意：您必须具备 root 特权才能进行这些更改操作。

1. 输入以下命令：

   `init 3`（如果需要，请切换到文本方式）

   `rmmod mousedev`（卸装鼠标设备驱动程序）

2. 将以下语句添加到用户主目录中的 .xinitrc 中：

   `xset m 1 1`（关闭鼠标加速）

3. 将以下语句添加到 /etc/modules.conf 中：

   `options mousedev xres=`*x* `yres=`*y*（将视频分辨率通知鼠标设备驱动程序），其中 *x* 和 y 指定视频分辨率

4. 输入以下命令：

   `insmod mousedev`（重新装入鼠标设备驱动程序）

   `init 5`（如果需要，返回 GUI 方式）

固件更新

Update Blade Firmware

To update a firmware component, select a target blade and a firmware file, and click "Update".

Target Blade1 - SN#229X7P J1NN

Firmware file Browse...

Update

选择固件更新对刀片服务器上的服务处理器固件进行更新。选择目标刀片服务器和用于更新的固件文件；然后单击更新。您可以从位于 http://www.ibm.com/pc/support/ 的 IBM Support Web 站点获取固件文件。

配置

Blade Server Configuration

Use the following links to jump down to different sections on this page.

Blade Information
Blade Policy Settings
Boot Sequence

Blade Information

Bay	Name
1	SN#K10V73621EB
2	
3	Blade 04
4	
5	SN#K10V7363140
6	SN#K10UJ353166
7	*No blade present*
8	SN#K10V7364105

选择 “ 配置 ” 选项来执行以下任务：

- 为刀片服务器定义名称。
- 启用或禁用 BladeCenter T 单元中所有刀片服务器上的以下项：
  - 本地电源控制
  - 本地 KVM 控制
  - 本地介质托盘控制
  - Wake on LAN 功能
- 查看或定义一台或多台刀片服务器的启动（引导）顺序。启动顺序对刀片服务器的以下引导记录源进行优先级安排：
  - 硬盘驱动器（0 至 3）。硬盘驱动器的选择取决于您的刀片服务器中安装的硬盘驱动器。
  - CD-ROM。
  - 网络 － PXE。选择 “ 网络 － PXE ” 将在下次开启或重新启动刀片服务器时尝试 PXE/DHCP 网络启动。

注：要将 CD-ROM 驱动器用作刀片服务器的引导记录源，必须已将刀片服务器指定为 CD-ROM 驱动器和 USB 端口的所有者。您可以通过按下刀片服务器上的 CD／软盘／USB 选择按键或通过第 25 页的『远程控制』中描述的远程控制选项来设置所有权。

Serial Over LAN

Serial Over LAN (SOL)

Use the following links to jump down to different sections on this page.

Serial Over LAN Configuration
Serial Over LAN Status

Serial Over LAN Configuration

Serial over LAN Enabled
SOL VLAN ID 4095
BSMP IP address range 10.10.10.80

Transport Parameters

Accumulate timeout 5 msec
Send threshold 250 bytes
Retry count 3
Retry interval 250 msec

Save

选择 **Serial over LAN** 来查看和更改 BladeCenter T 单元中所有的刀片服务器使用的全局 Serial over LAN（SOL）设置，启用或禁用 BladeCenter T 单元的全局 SOL。

Serial Over LAN Status

Click the checkboxes in the first column to select one or more blade servers; then, click one of the links below the table to enable or disable SOL on the selected blades.

Note: You have to enable the global "Serial over LAN" flag above before enabling SOL on individual blade servers.

☐	Bay	Name	SOL	SOL Session	BSMP IP Address
	1 2	*Blade does not suppport SOL*	n/a	n/a	n/a
	3 4	*Blade does not suppport SOL*	n/a	n/a	n/a
	5	*Blade does not suppport SOL*	n/a	n/a	n/a
	6	*Blade does not suppport SOL*	n/a	n/a	n/a
	7	*No blade present*			
	8	*Blade does not suppport SOL*	n/a	n/a	n/a

Disable Serial Over LAN
Enable Serial Over LAN

选择此选项同时监控每台刀片服务器的 SOL 状态并启用或禁用每台刀片服务器及 BladeCenter T 单元的全局 SOL。全局启用或禁用 SOL 不会影响每台刀片服务器的 SOL 会话状态；必须为 BladeCenter T 单元全局启用 SOL 并为准备启动 SOL 会话的每台刀片服务器单独启用 SOL。在缺省情况下，将全局启用 SOL 并对刀片服务器启用 SOL。

使用管理模块命令行界面启动并运行 SOL 会话。有关信息和说明，请参阅《*IBM @server BladeCenter 管理模块命令行界面参考大全*》。

I/O 模块任务

选择“ I/O 模块任务 ”部分中的选项来查看和更改 BladeCenter T 单元中网络接口 I/O 模块的设置或配置。

注：对于某些类型的 I/O 模块（如 pass-thru 模块），部分选项不适用并且不可用。

电源／重新启动

I/O Module Power/Restart

Select one or more module(s) using the checkboxes in the first column and then click on one of the links below the table to perform the desired action.

☐	Bay	Type	MAC Address	IP Address	Pwr	Details
☐	1	Ethernet SM	00:05:5D:89:A3:A0	10.90.90.94	On	POST results not complete: A0
	2		*No module*			
	3		*No module*			
	4		*No module*			

Power On Module(s)
Power Off Module(s)
Restart Module(s) and Run Standard Diagnostics
Restart Module(s) and Run Extended Diagnostics
Restart Module(s) and Run Full Diagnostics

选择电源／重新启动来显示 I/O 模块的电源状态并执行以下操作：

- 开启或关闭一个 I/O 模块
- 重置一个 I/O 模块

管理

I/O Module Management

Use the following links to jump down to different sections on this page.

Bay 1
Bay 2
Bay 3
Bay 4

Bay 1 (Ethernet SM)*

Current IP Configuration

Configuration method: Static
IP address: 192.168.70.127
Subnet mask: 255.255.255.0
Gateway address: 0.0.0.0

New Static IP Configuration

Status: Enabled

To change the IP configuration for this switch module, fill in the following fields and click "Save". This will save and enable the new IP configuration.

IP address: 192.168.70.127
Subnet mask: 255.255.255.0
Gateway address: 0.0.0.0

Advanced Management

选择管理来查看或更改 I/O 模块的 IP 配置、启用 I/O 模块端口、启用外部管理、ping I/O 模块、配置其它 I/O 模块高级设置、将 I/O 模块恢复为缺省配置并启动可能存在于 I/O 模块中的配置和管理固件。

注：I/O 模块固件出厂时定义的初始用户标识和密码如下：

- 用户标识：USERID（全部为大写字母）
- 密码：PASSW0RD（注意“PASSW0RD”中的零，而不是字母“O”）

有关基本 I/O 模块配置的更多信息，请参阅您的 BladeCenter T 单元的《*安装和用户指南*》。有关 I/O 模块的配置和管理固件的详细信息，请参阅 I/O 模块随附的文档。IBM *BladeCenter T 文档* CD 上提供某些 I/O 模块的文档。

固件更新

Update I/O Module Firmware

To update a firmware component, select a target module and a firmware file, and click "Update".

Target None of the I/O modules support flashing over this interface

Firmware file Browse...

Update

选择固件更新对 I/O 模块中的固件进行更新。选择目标 I/O 模块和用于更新的固件文件；然后单击更新。您可以从位于 http://www.ibm.com/pc/support/ 的 IBM Support Web 站点获取固件文件。

MM 控制

选择 **MM** 控制部分中的选项来查看和更改您通过管理模块 Web 界面会话登录到的（主要管理模块）管理模块的设置或配置。如果您的 BladeCenter T 单元配备了冗余管理模块，主要管理模块的配置设置将自动传送到辅助管理模块。

管理模块配置包括以下各项：
- 管理模块的名称
- 最多 12 个用于登录到管理模块中的登录概要文件
- 管理模块使用的端口
- 警报的处理方式
- 用于远程控制台以及与 I/O 模块进行通信的管理模块以太网连接
- SNMP、DNS、SMTP 和 LDAP 协议的设置
- 安全套接字层（SSL）和 Secure Shell（SSH）安全性的设置

这还包括执行以下任务：
- 备份和恢复管理模块配置
- 更新管理模块固件
- 恢复缺省配置
- 重新启动管理模块
- 从当前的活动管理模块切换到冗余管理模块

常规设置

View Configuration Summary

MM Information

Name SN#01
Contact No Contact Configured
Location No Location Configured

MM Date and Time

Date (mm/dd/yyyy): 02/26/2004
Time (hh:mm:ss): 11:32:33

Set MM Date and Time

Save

选择常规设置来查看或更改以下设置：

- 管理模块的名称
- 负责管理模块的联系人的姓名
- 管理模块的物理位置
- 管理模块中的实时时钟设置

SNMP 和 SMTP 配置过程中使用部分常规设置。请参阅第 40 页的『配置 SNMP』和第 42 页的『配置 SMTP』以获取其它信息。

登录概要文件

View Configuration Summary

Management Module Login Configuration

Use the following links to jump down to different sections on this page.
Login Profiles
Global Login Settings

Login Profiles

To configure a login profile, click a link in the "Login ID" column.

	Login ID	Access
1.	USERID	Read/Write
2.	USERID2	Read/Write
3.	belize	Read/Write
4.	spain	Read/Write
5.	france	Read/Write
6.	germany	Read/Write
7.	~ not used ~	
8.	~ not used ~	
9.	~ not used ~	
10.	~ not used ~	
11.	~ not used ~	
12.	~ not used ~	

选择登录概要文件来配置最多 12 个用于登录到管理模块中的概要文件；并指定以下全局登录设置：

- 用户认证方法（本地和／或 LDAP）

- 如何处理使用调制解调器登录的用户
- 五次失败登录尝试后的锁定期

Global Login Settings

These settings apply to all login profiles.

User authentication method: Local only

Logins through a modem connection: Disabled

Lockout period after 5 login failures: 2 minutes

为每个用户概要文件指定以下值：

- 登录标识
- 权限级别（缺省级别为只读）
- 密码（需要确认）

View Configuration Summary

Login Profile 1

Login ID: USERID

Password

Confirm password

Authority Level

- Supervisor
- Read-Only
- Custom
  - User Account Management
  - Blade Server Remote Console Access
  - Blade Server Remote Console and Virtual Media Access
  - Blade and I/O Module Power/Restart Access
  - Ability to Clear Event Logs
  - Basic Configuration (MM, I/O Modules, Blades)
  - Networking & Security Configuration
  - Advanced Configuration (MM, I/O Modules, Blades)

Configure SNMPv3 User

提供几种权限级别，每种级别赋予用户对不同管理模块功能区域的写访问权和执行访问权。可以赋予每个用户多个权限级别。具有“ 超级用户 ”权限的用户对所有管理模块功能具有写访问权和执行访问权。具有只读权限的用户只能查看所有管理模块功能。

警告： 如果您更改了管理模块上的缺省登录概要文件，请务必妥善保存登录标识和密码的记录。如果您忘记了管理模块登录标识和密码，则必须替换这个管理模块。

单击查看配置摘要以显示所有 BladeCenter T 用户和组件的配置设置。

警报

选择警报来指定监控哪些事件（从严重、警告和系统警报列表中选择）、将哪些事件通知发送给谁、事件通知的发送方式（SNMP 还是电子邮件）、通知是否包含事件日志以及其它警报参数。

端口指定

选择端口指定来配置管理模块使用的一些端口。表 3 中列出了可以在“端口指定”页面中配置的管理模块端口。

表 3. 用户可配置的管理模块端口

端口名称	缺省端口号	描述
HTTP	80	用于使用 UDP 的 Web 服务器 HTTP 连接的端口
HTTPS	443	用于使用 TCP 的 SSL 连接的端口

表 3. 用户可配置的管理模块端口 (续)

端口名称	缺省端口号	描述
Telnet	23	用于 Telnet 命令行界面连接的端口
SSH	22	用于 Secure Shell（SSH）命令行界面连接的端口
SNMP 代理	161	用于使用 UDP 的 SNMP get/set 命令的端口
SNMP 陷阱	162	用于使用 UDP 的 SNMP 陷阱的端口

表 4 中列出了管理模块使用的其它端口。这些端口是固定的并且无法修改。

表 4. 固定的管理模块端口

端口号（固定）	描述
25	用于 TCP 电子邮件警报的端口
53	用于 UDP 域名服务器（DNS）解析器的端口
68	用于使用 UDP 的 DHCP 客户机连接的端口
427	用于 UDP 服务位置协议（SLP）连接的端口
1044	用于远程磁盘功能的端口
1045	用于持久远程磁盘（卡载磁盘）的端口
5900	用于 TCP VNC 服务器 applet 的端口

单击查看配置摘要以显示所有 BladeCenter T 用户和组件的配置设置。

网络接口

View Configuration Summary

Management Module Network Interfaces

Use the following links to jump down to different sections on this page.

External Network Interface (eth0)

Internal Network Interface (eth1)

TCP Log

External Network Interface (eth0)

Interface: Enabled

DHCP: Try DHCP server. If it fails, use static IP config.

*** Currently the static IP configuartion is active for this interface.

*** This static configuration is shown below.

Hostname: MM0004230000B8

Static IP Configuration

IP address: 192.168.70.125

Subnet mask: 255.255.255.0

Gateway address: 0.0.0.0

选择网络接口来配置两个管理模块以太网接口：外部（远程管理和控制台）和内部（与 I/O 模块进行通信）。您也可以选择这个选项来查看 TCP 日志。

使用管理模块 Web 界面来更新 I/O 模块配置时，管理模块固件仅将其 I/O 模块的设置写到管理模块 NVRAM，而不会将其 I/O 模块的设置写到 I/O 模块 NVRAM。

如果 I/O 模块在管理模块无法应用其 NVRAM 中为 I/O 模块提供的 IP 地址时重新启动，I/O 模块将使用自己的 NVRAM 中的任意一个 IP 地址。如果两个 IP 地址不一样，您可能无法再管理 I/O 模块。管理模块无法在以下任何一种情况下从自己的 NVRAM 中应用 I/O 模块 IP 地址：

- 管理模块正在重新启动。
- 管理模块发生故障。
- 已从 BladeCenter T 单元中卸下管理模块。

您必须使用 Telnet 界面登录到 I/O 模块中，更改 IP 地址使它与您通过管理模块指定的那个保持一致，然后在 Telnet 会话中保存 I/O 模块设置（基本设置 → 保存更改）。

要使 I/O 模块能够与远程管理站通过管理模块外部以太网端口进行通信，I/O 模块内部网络接口以及管理模块内部和外部接口必须在同一子网中。

- 单击外部网络接口（**eth0**）时，将显示有关远程管理和控制台端口的接口信息：

  注：如果您准备使用冗余管理模块并希望两个模块使用相同的外部 IP 地址，请禁用 DHCP 并配置使用一个静态 IP 地址。（IP 配置信息将根据需要自动传送到冗余管理模块。）

  – 接口 － 以太网连接的状态（启用或禁用）。缺省值为 “ 启用 ”。
  – **DHCP** － 选择以下选项中的一种：
    - 尝试 **DHCP** 服务器。如果尝试失败，则使用静态 **IP** 配置（缺省值）
    - 启用 － 从 **DHCP** 服务器获取 **IP** 配置
    - 禁用 － 使用静态 **IP** 配置
  – 主机名 －（可选）这是您要用于管理模块的 IP 主机名（最多 63 个字符）。
  – 静态 **IP** 配置 － 仅当禁用 DHCP 时配置这一信息。
    - **IP** 地址 － 管理模块的 IP 地址必须包含从 0 至 255 的四个整数并以句点分隔（不能包含空格或连续的句点）。缺省设置为 192.168.70.125。
    - 子网掩码 － 子网掩码必须包含从 0 至 255 的四个整数并以句点分隔（不能包含空格）。缺省设置为 255.255.255.0。
    - 网关地址 － 网络网关路由器的 IP 地址必须包含从 0 至 255 的四个整数并以句点分隔（不能包含空格）。

- 单击内部网络接口（**eth1**）时，将显示与网络接口 I/O 模块（例如：以太网 I/O 模块或光纤通道 I/O 模块）通信的接口的相关信息。使用它执行以下任务：
  - 指定用于这个接口的 IP 地址。内部网络接口（eth1）和外部网络接口（eth0）必须在同一子网中。
  - 查看这个接口的数据率、双工方式、最大传输单元（MTU）、本地管理的 MAC 地址和内建 MAC 地址。您可以配置本地管理的 MAC 地址；其它字段是只读字段。
- 单击 **TCP** 日志查看当前存储在管理模块 TCP 日志中的条目。此日志包含管理模块上运行的 TCP/IP 代码生成的错误和警告消息；服务代表可以将它用于高级故障诊断。日志首先显示最新的条目。

  您可以对事件日志中的条目进行排序和过滤。

单击查看配置摘要以显示所有 BladeCenter T 用户和组件的配置设置。

网络协议

View Configuration Summary

Management Module Network Protocols

Use the following links to jump down to different sections on this page.
Simple Network Management Protocol (SNMP)
Domain Name System (DNS)
Simple Mail Transfer Protocol (SMTP)
Lightweight Directory Access Protocol (LDAP)

Simple Network Management Protocol (SNMP)

SNMP agent Enabled
SNMP traps Enabled

Community Name	Access Type		Host Name or IP Address
public	Set	1.	192.168.70.100
		2.	
		3.	
private	Set	1.	192.168.70.100
		2.	
		3.	

选择网络协议来查看或更改 SNMP、DNS、SMTP 和 LDAP 协议的设置。

单击查看配置摘要以显示所有 BladeCenter T 用户和组件的配置设置。

SNMP、SMTP 和 LDAP 配置过程中将使用部分网络协议设置。有关其它信息，请参阅第 40 页的『配置 SNMP』、第 42 页的『配置 SMTP』和第 42 页的『配置 LDAP』。

安全性

选择安全性来查看或更改 Web 服务器和 LDAP 客户机的安全套接字层（SSL）设置，查看或更改 Web 服务器 Secure Shell（SSH）设置。您可以启用或禁用（缺省）SSL 并选择使用自签署证书还是认证中心（CA）提供的证书。您还可以启用或禁用（缺省）SSH 并生成和管理 SSH 服务器密钥。

SSL、LDAP 和 SSH 配置中将使用部分安全性设置。请参阅第 47 页的『安全 Web 服务器和安全 LDAP』和第 57 页的『配置 Secure Shell 服务器』以获取其它信息。

配置文件

Backup MM Configuration

To backup the configuration, click "Backup." You can view the current configuration summary before backing it up.

Backup

Restore MM Configuration

To restore the MM configuration, select a file and click "Restore." To modify the configuration and then restore it, select a file and click "Modify & Restore."

Select configuration file to restore

Browse...

Restore   Modify and Restore

选择配置文件以备份或恢复管理模块配置文件。请参阅第 60 页的『使用配置文件』以获得相应的说明。

固件更新

Update MM Firmware

To update a firmware component on the MM, select a firmware file and click "Update". If there is a redundant MM installed, the firmware on the redundant MM will be automatically updated to the same level.

Browse...

Note: To ensure proper operation of the management module, make sure you update all MM firmware components to the same level.

Update

选择固件更新以更新管理模块固件；如果安装了第二个管理模块，固件更新将自动应用到两个管理模块。单击浏览找到所需的固件文件；然后单击更新。

管理模块固件共有几个需要独立安装的单独文件；必须安装所有的固件更新文件。您可以从位于 http://www.ibm.com/pc/support/ 的 IBM Support Web 站点获取固件文件。

恢复缺省配置

Restore Defaults

This action will cause all MM settings to be set to factory defaults.

You will lose your TCP/IP connection as a result. You will need to reconfigure the external network interface to restore connectivity.

Clearing of the MM configuration will be followed by a restart of the MM.
Press "Restore Defaults" button if you want to proceed.

Restore Defaults

选择恢复缺省配置将管理模块恢复为出厂缺省配置。

重新启动 **MM**

Restart MM

This action will be followed by a restart of the MM. All existing network connections will be temporarily lost as a result. You will need to open a new browser and relogin to get back in to the user interface. Click "Restart" if you want to continue and restart the MM.

Restart

Switch Over to Redundant MM

This action will cause a restart of this MM, followed by a switch over to the redundant MM in bay 2. All existing network connections will be temporarily lost as a result. You will need to open a new browser and relogin to get back in to the user interface. You will also need to move the video, mouse, and keyboard cables to the redundant MM. Click "Switch Over" if you want to continue and switch over to the redundant MM.

Note: If you have DHCP enabled on the primary MM's external network interface, and the IP address is assigned by the DHCP server, after the switch over to the redundant MM, the DHCP server will assign a different IP address to the redundant MM. If you want to be able to access both MMs at the same static IP address, you need to disable DHCP. Static IP configuration is the recommended setting in this environment.

Switch Over

选择重新启动 **MM** 以重新启动（重置）管理模块。如果安装了第二个管理模块，请选择此选项以更改到冗余管理模块。

网络和安全性配置

以下部分描述了如何配置下列各项的管理模块联网和安全性参数：

- SNMP 和 DNS（请参阅『配置 SNMP』）
- SMTP（请参阅第 42 页的『配置 SMTP』）
- SSL 和 LDAP（请参阅第 42 页的『配置 LDAP』）
- SSH（请参阅第 57 页的『配置 Secure Shell 服务器』）

配置 **SNMP**

您可以通过查询 SNMP 代理收集 sysgroup 信息并将已配置的 SNMP 警报发送到已配置的主机名或 IP 地址。

注：如果您准备在管理管理上配置简单网络管理协议（SNMP）陷阱，则必须在 SNMP 管理器上安装并编译管理信息基础（MIB）。MIB 支持 SNMP 陷阱。您从 IBM Support Web 站点下载的管理模块固件更新软件包中包含此 MIB。

完成以下步骤以配置 SNMP：

1. 登录到您要在其中配置 SNMP 的管理模块。有关更多信息，请参阅第 16 页的『启动管理模块 Web 界面』。
2. 在导航窗格中，单击 **MM** 控制 → 常规设置。在打开的管理模块信息页面中，指定以下信息：
   - 管理模块名称 － 用于识别管理模块的名称。电子邮件和 SNMP 警报通知中将包含此名称以帮助您识别警报来源。
   - 系统联系人 － BladeCenter T 单元出现问题时，联系人的姓名和电话号码。

- 系统位置 — 快速找到 BladeCenter T 单元位置以进行维护或其它操作的充足的详细信息。

3. 滚动到页面底部并单击保存。
4. 在导航窗格中，单击 **MM** 控制 → 网络协议；然后单击简单网络管理协议（**SNMP**）链接。将显示一个类似于下图的页面。
5. 选择 **SNMP** 代理和 **SNMP** 陷阱字段中的启用将警报转发到您网络中的 SNMP 团体。要启用 SNMP 代理，必须满足以下条件：
   - 必须在“常规设置”页面中指定系统联系人。
   - 必须在“常规设置”页面中指定系统位置。
   - 至少必须指定一个团体名称。
   - 至少必须为该团体指定一个有效的 IP 地址或主机名（如果已启用 DNS）。

   注：通知方法为 SNMP 的警报接收方将无法接收警报，直至同时启用 SNMP 代理和 SNMP 陷阱。
6. 设置一个团体来定义 SNMP 代理和 SNMP 管理器之间的管理关系。您至少必须定义一个团体。每个团体定义包含以下参数：
   - 名称
   - IP 地址

   只要其中一个参数不正确就无法进行 SNMP 管理访问。

   注：如果出现错误消息窗口，请对错误窗口中列出的字段进行必要的调整。然后滚动到页面底部并单击保存以保存纠正的信息。您至少必须配置一个团体才能启用此 SNMP 代理。
7. 在团体名称字段中，输入一个名称或认证字符串以指定该团体。
8. 在对应的主机名或 **IP** 地址字段中，输入每个团体管理器的主机名或 IP 地址。
9. 如果您的网络中没有 DNS 服务器，请滚动到页面底部并单击保存。

10. 如果您的网络中有 DNS 服务器，请滚动到域名系统（**DNS**）部分。将显示一个类似于下图的页面。

Domain Name System (DNS)

DNS Disabled

DNS server IP address 1 0.0.0.0

DNS server IP address 2 0.0.0.0

DNS server IP address 3 0.0.0.0

11. 如果您的网络中有一台（或多台）DNS 服务器，请选择 **DNS** 字段中的启用。**DNS** 字段指定了您是否在网络中使用 DNS 服务器将主机名转换为 IP 地址。
12. （可选）如果您已启用 DNS，请在 **DNS** 服务器 **IP** 地址字段中指定您网络中的 DNS 服务器 IP 地址（最多三台 DNS 服务器）。每个 IP 地址必须包含从 0 至 255 的整数并以句点分隔。
13. 滚动到页面底部并单击保存。
14. 在导航窗格中，单击 **MM** 控制 → 重新启动 **MM** 以激活更改。

配置 SMTP

完成以下步骤以指定简单邮件传输协议（SMTP）服务器的 IP 地址或主机名。

注：如果您准备为电子邮件警报通知设置 SMTP 服务器，确保 **MM** 控制 → 常规设置页面中的 **MM** 信息部分中的名称字段中的名称是电子邮件地址的一个有效部分（例如：不包含空格）。

1. 登录到您要在其中配置 SMTP 的管理模块。有关更多信息，请参阅第 16 页的『启动管理模块 Web 界面』。
2. 在导航窗格中，单击 **MM** 控制 → 网络协议并向下滚动到简单邮件传输协议（**SMTP**）部分。

Simple Mail Transfer Protocol (SMTP)

SMTP server host name or IP address

3. 在 **SMTP** 服务器主机名或 **IP** 地址字段中，输入 SMTP 服务器的主机名。使用此字段指定 SMTP 服务器的 IP 地址或主机名（如果已启用并配置了 DNS）。
4. 滚动到页面底部并单击保存。

配置 LDAP

使用轻量级目录访问协议（LDAP）服务器，管理模块可以通过在 LDAP 服务器上查询和搜索 LDAP 目录，而不必搜索其本地用户数据库对用户进行认证。然后，所有 LDAP 客户机（BladeCenter T 管理模块或服务器远程管理适配器）可以通过中央 LDAP 服务器对任何用户访问进行远程认证。这需要在管理模块上提供 LDAP 客户机支持。您也可以根据在 LDAP 服务器上找到的信息来指定权限级别。

除了常规的用户（口令检查）认证外，您也可以使用 LDAP 将用户和管理模块指定到组并执行组认证。例如，一个管理模块可以与一个或多个组相关联，如果用户至少属于一个与管理模块相关联的组，他只能通过组认证。

设置客户机以使用 LDAP 服务器

请完成以下步骤来设置客户机以使用 LDAP 服务器：

1. 登录到您要在其中设置客户机的管理模块。有关更多信息，请参阅第 16 页的『启动管理模块 Web 界面』。
2. 在导航窗格中，单击 **MM 控制** → 网络协议。向下滚动到轻量级目录访问协议（**LDAP**）客户机部分。将显示一个类似于下图的页面。

Lightweight Directory Access Protocol (LDAP) Client

Pre-Configured LDAP Servers

LDAP Server Port
1.
2.
3.

Miscellaneous Parameters

Root DN
User Search Base DN
Group Filter RSA*
Binding Method User Principal Name

Set DN and password only if Binding Method used is Client Authentication

Set attribute names for LDAP client search algorithm

Save

3. 使用以下信息配置 LDAP 客户机：

LDAP 服务器

管理模块包含一个 V2.0 LDAP 客户机，您可以对它进行配置通过位于中央的 LDAP 服务器提供认证。您最多可以配置三台 LDAP 服务器。每台服务器的端口号是可选的。如果该字段留空，将对非安全 LDAP 连接使用缺省值 389。对于安全连接，缺省值为 636。您至少必须配置一台 LDAP 服务器。

根 DN 这是 LDAP 服务器上目录树的根条目的专有名称（例如：dn=companyABC,dn=com）。

用户搜索基本 DN

作为用户认证过程的一部分，必须在 LDAP 服务器上搜索一个或多个与特定用户关联的属性。任何搜索请求必须指定实际搜索的基本专有名称。用户搜索基本 **DN** 字段指定了用于搜索用户目录的基本专有名称（例如：cn=Users,dn=companyABC,dn=com）。如果该字段留空，则根专有名称将作为搜索基本。

用户搜索是认证过程的一部分。通过执行用户搜索来检索用户的相关信息，如登录许可权、回拨号和组员身份。对于 V2.0 LDAP 客户机，必须配置此参数；否则使用根专有名称的搜索可能会失败（如 Microsoft Windows® Server 2003 Active Directory 服务器上发现的情况那样）。

ASM 组过滤条件

此参数用于组认证。它指定管理模块所属的一系列组。如果该字段留空，将禁用组认证。否则，将使用这个过滤条件执行组认证。指定的过滤条件可以是一个特定的组名（例如：RSAWest）、一个带前缀的通配符（例

如：RSA*）或一个通配符（以 * 指定)。如果使用一个特定名称，管理模块将仅属于该组。如果使用前缀过滤条件（例如：RSA*），管理模块将属于开头三个字母为 RSA 的所有组。如果使用通配符过滤条件（*），管理模块将属于所有组。缺省过滤条件是 RSA*。

在用户认证（期间会验证用户标识和密码）后进行组认证。组认证是指验证用户是否至少是一个与管理模块关联的组的成员的过程。例如，如果组过滤条件设置为 RSA* 并且用户属于两个组（例如：Engineering 和 RSAWest），则通过组认证，因为用户属于与过滤条件 RSA* 匹配的组（RSAWest)。如果用户所属的组与过滤条件都不匹配，则组认证失败并且不允许用户访问管理模块。请注意，如果组过滤条件是 *，组认证将自动通过，因为用户所属的任何组都与此通配符匹配。

绑定方法

对于用户认证过程中与 LDAP 服务器的初始绑定，请选择以下一个选项：

匿名认证。在没有客户机专有名称或密码的情况下尝试绑定。如果绑定成功，将请求在 LDAP 服务器上为尝试登录的用户搜索一个条目。如果找到条目，将进行第二次绑定尝试，这一次将使用用户的专有名称和密码。如果尝试成功，用户通过用户认证阶段。如果启用组认证，随后将尝试它。

客户机认证。将使用该配置参数指定的客户机专有名称和密码尝试绑定。如果绑定成功，用户认证阶段将如匿名认证中类似的步骤进行下去。

用户主体名称。将使用登录过程中使用的凭证直接尝试绑定。如果尝试成功，用户通过用户认证阶段。用户主体名称通常是指一个标准名称，如 johndoe@abc.com。但是，johndoe 也是可接受的。

严格用户主体名称。它类似于用户主体名称，唯一的区别在于用户必须输入标准名称。即 johndoe@abc.com 是可接受的，而 johndoe 则是不可接受的。将对用户输入的名称中的 @ 符号进行语法分析。

配置 LDAP 客户机认证

请完成以下步骤来配置 LDAP 客户机认证：

1. 在导航窗格中，单击 **MM** 控制 → 网络协议。
2. 向下滚动到轻量级目录访问协议（**LDAP**）客户机部分并单击设置客户机认证的 **DN** 和密码。将显示一个类似于下图的页面。
3. 在用户认证过程中使用匿名认证、基于客户机的认证或用户主体名称执行与 LDAP 服务器的初始绑定。要使用基于客户机的认证，请在客户机 **DN** 字段中输入客户机专有名称。在密码字段中输入密码或将它留空。

配置 LDAP 搜索属性

请完成以下步骤来配置 LDAP 搜索属性：

1. 在导航窗格中，单击 **MM 控制** → **网络协议**。
2. 向下滚动到轻量级目录访问协议（**LDAP**）客户机部分并单击**设置基于 LDAP 认证的搜索属性名称**。将显示一个类似于下图的页面。

View Configuration Summary

LDAP Search Attributes

UID Search Attribute
Group Search Attribute
Login Permission Attribute

Clear All Fields | Cancel | Save

3. 要配置搜索属性，请使用以下信息：

UID 搜索属性

当选定的绑定方法是匿名认证或客户机认证时，与 LDAP 服务器进行初始绑定后将执行搜索请求以检索有关用户的特定信息，包括专有名称、登录许可权和用户的组员身份。要检索这一信息，搜索请求必须指定用于表示该服务器上用户标识的属性名称。具体而言，该名称将作为用户输入的登录标识的搜索过滤条件。在这里配置该属性名称。如果该字段留空，在用户认证期间将使用缺省 UID。例如，在 Active Directory 服务器上，用户标识的常用属性名称是 sAMAccoutName。

当选定的绑定方法是用户主体名称或严格主体名称时，如果输入的用户标识采用*用户标识@某域*格式，则在用户认证过程中，**UID** 搜索属性字段缺省值将自动使用 userPrincipalName。

组搜索属性

当配置组过滤条件名称时，必须从 LDAP 服务器检索用户所属的组的列表。这是执行组认证所必需的。要检索该列表，发送到服务器的搜索过滤条件必须指定与组关联的属性名称。该字段指定了这个属性名称。

如果该字段留空，过滤条件中的属性名称缺省使用 memberOf。

登录许可权属性

当用户使用 LDAP 服务器成功通过认证时，必须检索用户的登录许可权。要检索这些许可权，发送到服务器的搜索过滤条件必须指定与登录许可权关联的属性名称。该字段指定了这个属性名称。

如果该字段留空，将授予用户缺省的只读许可权并假定通过用户和组认证。检索成功时，LDAP 服务器返回的属性值将根据以下信息进行解释：

- 它必须是一个以 12 个连续的零或壹格式输入的二进制位串，其中每个位代表一组特殊的功能（例如：010000000000 或 0000110010000）。根据每个位的位置进行编号。最左侧的位是第 0 位，而最右侧的位是第 11 位。特定位置的值 “ 1 ” 将启用相应的功能。而值 “ 0 ” 将禁用该功能。以下是与 12 个位置相关的不同功能：
  - 始终拒绝（第 0 位）：如果设置此位，用户将始终无法通过认证。此功能可用于阻止与特定组相关联的一个或多个特定用户。
  - 超级用户访问权（第 1 位）：如果设置此位，将授予用户管理员特权。用户对每个功能都具有读写访问权。如果设置此位，则无需逐个设置第 2 位至第 12 位。
  - 只读访问权（第 2 位）：如果设置此位，用户具有只读访问权并且不能执行任何维护操作（例如：重新启动、远程操作和固件更新），也不能（使用保存、清除或恢复功能）修改任何内容。请注意，只读和其它位是互斥的并且第 2 位的优先级最低。即如果设置了任何其它位，将忽略第 2 位。
  - 联网和安全性（第 3 位）：如果设置此位，用户可以修改 “ MM 控制 ” 的 “ 安全性 ” 、 “ 网络协议 ” 和 “ 网络接口 ” 页面中的设置。如果设置此位，用户还可以修改 I/O 模块任务的 “ 管理 ” 页面中的设置。
  - 用户帐户管理（第 4 位）：如果设置此位，用户可以添加、修改和删除用户并更改 “ 登录概要文件 ” 页面中的 “ 全局登录设置 ”。

- 刀片服务器远程控制台访问权（第 5 位）：如果设置此位，用户可以访问远程服务器控制台。
- 刀片服务器远程控制台和虚拟介质访问权（第 6 位）：如果设置此位，用户可以访问远程服务器控制台和远程服务器的虚拟介质功能。
- 刀片和 I/O 模块电源／重新启动访问权（第 7 位）：如果设置此位，用户可以访问远程刀片服务器和 I/O 模块的开机和重新启动功能。“电源／重新启动”页面中提供这些功能。
- 基本配置（MM、I/O 模块、刀片）（第 8 位）：如果设置此位，用户可以修改“MM 控制”的“常规设置”和“警报”页面以及“刀片任务”的“配置”页面。
- 清除事件日志的能力（第 9 位）：如果设置此位，用户可以清除事件日志。所有人都可以查看事件日志，但这一特殊许可权是清除日志所必需的。
- 高级配置（MM、I/O 模块、刀片）（第 10 位）：如果设置此位，用户在配置管理模块、刀片服务器、I/O 模块和 VPD 时将不受限制。用户还可以在管理模块或刀片服务器上执行固件升级、将管理模块恢复为其出厂时的缺省设置、从配置文件修改并恢复管理模块的配置以及重新启动或重设管理模块。
- 保留（第 11 位）：此位保留以备将来使用。

• 如果不设置任何位，缺省情况是授予用户只读权限。
• 将优先级赋予直接从用户记录检索的登录许可权。如果用户记录没有登录许可权属性，将尝试从用户所属的组检索许可权。这将作为组认证阶段的一部分进行。将授予用户所有组的所有位的“或”权限。仅当所有其它位都设置为零时才设置“只读访问权”位。如果为任何组设置了“始终拒绝”位，将拒绝用户访问。“始终拒绝”位的优先级始终高于所有其它位。

安全 Web 服务器和安全 LDAP

安全套接字层（SSL）是一种提供通信隐私的安全协议。SSL 使得应用程序能以为防止窃听、篡改和消息伪造而设计的方式进行通信。

您可以配置管理模块对两种连接类型使用 SSL 支持：安全 Web 服务器（HTTPS）连接和安全 LDAP（LDAPS）连接。根据连接的类型，管理模块可以充当 SSL 客户机或 SSL 服务器。下表显示了管理模块充当安全 Web 服务器连接的 SSL 服务器。管理模块充当安全 LDAP 连接的 SSL 客户机。

表 5. 管理模块 SSL 连接支持

连接类型	**SSL** 客户机	**SSL** 服务器
安全 Web 服务器（HTTPS）	用户的 Web 浏览器（例如：Microsoft Internet Explorer）	管理模块 Web 服务器
安全 LDAP 连接（LDAPS）	管理模块 LDAP 客户机	LDAP 服务器

您可以从 **MM** 控制 → 安全性页面中查看或更改安全套接字层（SSL）设置。您可以启用或禁用 SSL 并管理 SSL 所需的证书。

配置安全性

使用本节中的常规步骤来配置管理模块 Web 服务器的安全性以及管理模块和 LDAP 服务器之间的连接的安全性。如果您不熟悉如何使用 SSL 证书，请阅读『SSL 证书概述』中的信息。

安全 Web 页面的内容是上下文相关的。当生成证书请求或证书签署请求时、导入或删除证书时以及为客户机或服务器启用或禁用 SSL 时，页面中提供的选项会更改。

使用以下常规任务列表为管理模块配置安全性：

1. 配置安全 Web 服务器：
   a. 禁用 SSL 服务器。请使用 **MM** 控制 → 安全性页面中的 **Web** 服务器的 **SSL** 服务器配置部分。
   b. 生成或导入证书。请使用 **MM** 控制 → 安全性页面中的 **SSL** 服务器证书管理部分。（请参阅第 49 页的『SSL 服务器证书管理』。）
   c. 启用 SSL 服务器。请使用 **MM** 控制 → 安全性页面中的 **Web** 服务器的 **SSL** 服务器配置部分。（请参阅第 55 页的『为安全 Web 服务器启用 SSL』。）
2. 为 LDAP 连接配置 SSL 安全性：
   a. 禁用 SSL 客户机。请使用 **MM** 控制 → 安全性页面中的 **LDAP** 客户机的 **SSL** 客户机配置部分。
   b. 生成或导入证书。请使用 **MM** 控制 → 安全性页面中的 **SSL** 客户机证书管理部分。（请参阅第 55 页的『SSL 客户机证书管理』。）
   c. 导入一个或多个受信任的证书。请使用 **MM** 控制 → 安全性页面中的 **SSL** 客户机受信任的证书管理部分。（请参阅第 55 页的『SSL 客户机受信任的证书管理』。）
   d. 启用 SSL 客户机。请使用 **MM** 控制 → 安全性页面中的 **LDAP** 客户机的 **SSL** 客户机配置部分。（请参阅第 57 页的『为 LDAP 客户机启用 SSL』。）
3. 重新启动管理模块以使 SSL 服务器配置更改生效。有关更多信息，请参阅第 40 页的『重新启动 MM』。

   注：对 SSL 客户机配置的更改将立即生效，而无需重新启动管理模块。

SSL 证书概述

您可以结合自签署证书或第三方认证中心签署的证书使用 SSL。使用自签署证书是使用 SSL 的最简单的方法，但它会带来一些安全性风险。风险产生的原因在于尝试客户机与服务器之间的第一次连接时，SSL 客户机无法验证 SSL 服务器的身份。第三方有可能冒充服务器并拦截管理模块与 Web 浏览器之间流动的数据。如果在浏览器与管理模块之间的第一次连接时，已将自签署证书导入浏览器的证书库，该浏览器的所有未来通信将是安全的（假定第一次连接未受到攻击）。

要获得更高的安全性，您可以使用认证中心签署的证书。要获取已签署的证书，请使用“ SSL 证书管理 ”页面来生成证书签署请求。您必须随后将证书签署请求发送到认证中心并安排证书获取事宜。接收到证书后，请使用导入已签署证书链接将它导入管理模块，随后即可启用 SSL。

认证中心的作用是验证管理模块的身份。证书包含认证中心和管理模块的数字签名。如果证书是由知名认证中心签发的或是已将认证中心的证书导入 Web 浏览器，浏览器可以确认证书并正确识别管理模块 Web 服务器。

管理模块需要两个证书，一个用于安全 Web 服务器，一个用于安全 LDAP 客户机。并且安全 LDAP 客户机需要一个或多个受信任的证书。安全 LDAP 客户机使用受信任的证书来正确识别 LDAP 服务器。受信任的证书是签署 LDAP 服务器证书的认证中心的证书。如果 LDAP 服务器使用自签署证书，受信任的证书可以是 LDAP 服务器自身的证书。如果您的配置中使用了多台 LDAP 服务器，则可以导入其它受信任的证书。

SSL 服务器证书管理

SSL 服务器要求在启用 SSL 之前安装一个有效证书和对应的专用加密密钥。有两种生成专用密钥和必需证书的方法：使用自签署证书以及使用认证中心签署的证书。如果您要对 SSL 服务器使用自签署证书，请参阅第 50 页的『生成自签署证书』。如果您要对 SSL 服务器使用认证中心签署的证书，请参阅第 51 页的『生成证书签署请求』。

生成自签署证书： 完成以下步骤以生成新的专用加密密钥和自签署证书：

1. 在导航窗格中，单击 **MM 控制** → **安全性**。将显示一个类似于下图的页面。

SSL Server Configuration for Web Server

SSL Server Disabled Save

SSL Server Certificate Management

SSL server certificate status: No certificate or certificate signing request (CSR) has been generated.

Generate a New Key and a Self-signed Certificate

Generate a New Key and a Certificate Signing Request (CSR)

SSL Client Configuration for LDAP Client

SSL Client Disabled Save

SSL Client Certificate Management

SSL client certificate status: No certificate or certificate signing request (CSR) has been generated.

Generate a New Key and a Self-signed Certificate

2. 在 **Web** 服务器的 **SSL** 服务器配置部分中，确保已禁用 SSL 服务器。如果尚未禁用它，请选择 **SSL** 服务器字段中的禁用，然后单击保存。
3. 在 **SSL** 服务器证书管理部分中，选择生成新密钥和自签署证书。将显示一个类似于下图的页面。

SSL Self-signed Certificate

Certificate Data

Country (2 letter code)

State or Province

City or Locality

Organization Name

MM Host Name

Contact Person

Email Address

Optional Certificate Data

Organizational Unit

Surname

Given Name

Initials

DN Qualifier

Generate Certificate

4. 在必填字段和适用于您的配置的可选字段中输入信息。有关这些字段的描述，请参阅第 51 页中的“必需的证书数据”。输入完信息后，请单击生成证书。将生成新的加密密钥和证书。这个过程可能需要几分钟的时间。

   将显示一个类似于下图的页面，它显示已安装一个自签署证书。

SSL Server Certificate Management

SSL server certificate status: A self-signed certificate is installed.

Generate a New Key and a Self-signed Certificate

Generate a New Key and a Certificate Signing Request (CSR)

生成证书签署请求： 完成以下步骤以生成新的专用加密密钥和证书签署请求：

1. 在导航窗格中，单击 **MM** 控制 → 安全性。
2. 在 **Web** 服务器的 **SSL** 服务器配置部分中，确保已禁用 SSL 服务器。如果尚未禁用它，请选择 **SSL** 服务器字段中的禁用，然后单击保存。
3. 在 **SSL** 服务器证书管理部分中，选择生成新的密钥和证书签署请求。将显示一个类似于下图的页面。

SSL Certificate Signing Request (CSR)

Certificate Request Data

Country (2 letter code)

State or Province

City or Locality

Organization Name

MM Host Name

Contact Person

Email Address

Optional Certificate Data

Organizational Unit

Surname

Given Name

Initials

DN Qualifier

CSR Attributes and Extension Attributes

Challenge Password

Unstructured Name

Generate CSR

4. 在必填字段和适用于您的配置的可选字段中输入信息。这些字段与自签署证书的字段相同并且添加了额外部分。

   以下部分描述了各个常见字段。

   必需的证书数据

   以下是生成自签署证书或证书签署请求必需的用户输入字段：

   国家或地区
   : 使用该字段表明管理模块所处的国家或地区。该字段必须包含 2 位字符的国家或地区代码。

   省／直辖市
   : 使用该字段表明管理模块所处的省／直辖市。该字段最多可以包含 30 个字符。

市／县／区
: 使用该字段表明管理模块所处的市／县／区。该字段最多可以包含 50 个字符。

组织名称
: 使用该字段表明拥有管理模块的公司或组织。当使用该信息生成证书签署请求时，签发证书的认证中心可以对请求证书的组织是否是指定公司或组织名称的合法拥有者进行验证。该字段最多可以包含 60 个字符。

MM 主机名
: 使用该字段表明当前显示在浏览器 Web 地址栏中的管理模块主机名。

  确保您在 **MM** 主机名字段中输入的值与 Web 浏览器知道的主机名完全匹配。浏览器将对解析后的 Web 地址中的主机名与证书中出现的名称进行比较。为避免浏览器发出证书警告，该字段中使用的值必须与浏览器用于连接管理模块的主机名匹配。例如，如果地址字段中的 Web 地址当前为 http://mm11.xyz.com/private/main.ssi，则用于 **MM** 主机名字段的值必须为 mm11.xyz.com。如果 Web 地址为 http://mm11/private/main.ssi，则使用的值必须为 mm11。 如果 Web 地址为 http://192.168.70.2/private/main.ssi，则使用的值必须为 192.168.70.2。

  该证书属性通常称为公共名称。

  该字段最多可以包含 60 个字符。

联系人
: 使用该字段表明负责管理模块的联系人的姓名。该字段最多可以包含 60 个字符。

电子邮件地址
: 使用该字段表明负责管理模块的联系人的电子邮件地址。该字段最多可以包含 60 个字符。

可选的证书数据

以下是生成自签署证书或证书签署请求可选的用户输入字段：

组织单位
: 使用该字段表明拥有管理模块的公司或组织的单位。该字段最多可以包含 60 个字符。

姓
: 使用该字段表明附加信息，如管理模块的负责人员的姓。该字段最多可以包含 60 个字符。

名
: 使用该字段表明附加信息，如管理模块的负责人员的名。该字段最多可以包含 60 个字符。

姓名首字母
: 使用该字段表明附加信息，如管理模块的负责人员的姓名首字母。该字段最多可以包含 20 个字符。

DN 限定符
: 使用该字段表明附加信息，如管理模块的专有名称限定符。该字段最多可以包含 60 个字符。

证书签署请求属性

以下字段是可选字段（除非您选定的认证中心要求它们）：

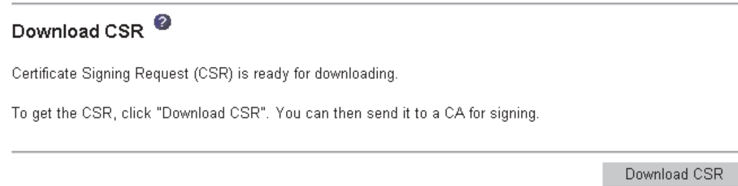
质询密码

使用该字段为证书签署请求指定密码。该字段最多可以包含 30 个字符。

无结构名称

使用该字段表明附加信息，如为管理模块指定的无结构名称。该字段最多可以包含 60 个字符。

5. 输入完信息后，请单击生成 **CSR**。将生成新的加密密钥和证书。这个过程可能需要几分钟的时间。当完成该步骤时，将显示一个类似于下图的页面。



6. 单击下载 **CSR**，然后单击保存将文件保存到工作站。您创建证书签署请求时生成的文件格式为 DER。如果您的认证中心要求数据采用其它格式（如 PEM），您可以使用 OpenSSL（http://www.openssl.org）等工具对文件进行转换。如果认证中心要求您将证书签署请求文件的内容复制到 Web 页面中，通常需要 PEM 格式。

使用 OpenSSL 将证书签署请求从 DER 格式转换为 PEM 格式的命令类似于以下命令：

```
openssl req -in csr.der -inform DER -out csr.pem -outform PEM
```

7. 将证书签署请求发送给您的认证中心。当认证中心发回已签署的证书时，您可能需要将它转换为 DER 格式。（如果您在电子邮件中或 Web 页面中接收到证书，它可能采用了 PEM 格式。）您可以使用认证中心提供的工具或 OpenSSL（http://www.openssl.org）等工具更改证书格式。将证书从 PEM 格式转换为 DER 格式的命令类似于以下命令：

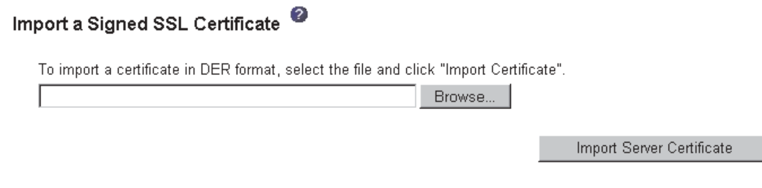
```
openssl x509 -in cert.pem -inform PEM -out cert.der -outform DER
```

认证中心发回已签署的证书后，请转至第 8 步。

8. 在导航窗格中，单击 **MM** 控制 → 安全性。滚动到“SSL 服务器证书管理”部分，它类似于下图中的页面。



9. 选择导入已签署的证书。将显示一个类似于下图的页面。



10. 单击浏览。
11. 单击所需的证书文件，然后单击打开。将在浏览按钮旁的字段中显示文件名（包含完整路径）。
12. 单击导入服务器证书以开始此过程。将文件传送到管理模块中的存储器时，将显示一个进度指示器。将继续显示该页面直至传送完成。

为安全 **Web** 服务器启用 **SSL**

注：要启用 SSL，您必须安装有效的 SSL 证书。

完成以下步骤以启用安全 Web 服务器：

1. 在导航窗格中，单击 **MM** 控制 → 安全性。显示的页面类似于下图，它显示已安装的有效 SSL 服务器证书。如果 SSL 服务器证书状态未显示已安装有效的 SSL 证书，请转至第 49 页的『SSL 服务器证书管理』。

   SSL Server Certificate Management

   SSL server certificate status: A CA-signed certificate is installed.

   Generate a New Key and a Self-signed Certificate

   Generate a New Key and a Certificate Signing Request (CSR)

2. 滚动到“Web 服务器的 SSL 服务器配置”部分并选择 **SSL** 客户机字段中的启用，然后单击保存。管理模块下次重新启动时，选定的值将生效。

SSL 客户机证书管理

SSL 客户机要求在启用 SSL 之前安装一个有效证书和对应的专用加密密钥。有两种生成专用密钥和必需证书的方法：使用自签署证书以及使用认证中心签署的证书。

为 SSL 客户机生成专用加密密钥和证书的过程与 SSL 服务器的过程相同，唯一的区别在于您使用的是安全 Web 页面的 **SSL** 客户机证书管理部分，而不是 **SSL** 服务器证书管理部分。如果您要为 SSL 客户机使用自签署证书，请参阅第 50 页的『生成自签署证书』。如果您要为 SSL 客户机使用认证中心签署的证书，请参阅第 51 页的『生成证书签署请求』。

SSL 客户机受信任的证书管理

安全 SSL 客户机（LDAP 客户机）使用受信任的证书来正确识别 LDAP 服务器。受信任的证书可以是签署 LDAP 服务器证书的认证中心的证书，也可以是 LDAP 服务器的实际证书。在启用 SSL 客户机之前，至少必须将一个证书导入管理模块。您最多可以导入三个受信任的证书。

完成以下步骤以导入受信任的证书：

1. 在导航窗格中，选择 **MM** 控制 → 安全性。
2. 在“LDAP 客户机的 SSL 客户机配置”部分中，确保已禁用 SSL 客户机。如果尚未禁用它，请选择 **SSL** 客户机字段中的禁用，然后单击保存。

3. 滚动到 **SSL** 客户机受信任的证书管理部分。将显示一个类似于下图的页面。

4. 单击受信任的 **CA** 证书 **1** 字段旁的导入。将显示一个类似于下图的页面。

5. 单击浏览。
6. 选择所需的证书文件，然后单击打开。将在浏览按钮旁的框中显示文件名（包含完整路径）。
7. 要开始导入进程，单击导入证书。将文件传送到管理模块中的存储器时，将显示一个进度指示器。将继续显示该页面直至传送完成。

MM 控制 → 安全性页面中的“ SSL 客户机受信任的证书管理 ”部分现在类似于下图。

受信任的 CA 证书 1 选项的删除按钮现已可用。如果要删除受信任的证书，请单击对应的删除按钮。

您可以使用受信任的 CA 证书 2 和受信任的 CA 证书 3 导入按钮导入其它受信任的证书。

为 **LDAP** 客户机启用 **SSL**

使用“安全性”页面的“LDAP 客户机的 SSL 客户机配置”部分来启用或禁用 LDAP 客户机的 SSL。要启用 SSL，您必须安装有效的 SSL 客户机证书以及至少一个受信任的证书。

完成以下步骤为客户机启用 SSL：

1. 在导航窗格中，单击 **MM** 控制 → 安全性。将显示一个类似于下图的页面。

   SSL Client Configuration for LDAP Client

   SSL Client Disabled Save

   SSL Server Certificate Management

   SSL server certificate status: A CA-signed certificate is installed.

   Generate a New Key and a Self-signed Certificate

   Generate a New Key and a Certificate Signing Request (CSR)

   SSL Client Trusted Certificate Management

   Trusted CA Certificate 1 Import Remove

   Trusted CA Certificate 2 Import

   Trusted CA Certificate 3 Import

   “MM 控制 → 安全性”页面将显示安装的 SSL 客户机证书和受信任的 CA 证书 1。
2. 在“LDAP 客户机的 SSL 客户机配置”页面中，选择 **SSL** 客户机字段中的启用。
3. 单击保存。选定的值将立即生效。

配置 **Secure Shell** 服务器

Secure Shell（SSH）功能提供了对命令行界面的安全访问以及管理模块的 Serial over LAN（命令行控制台）重定向功能。

通过交换 Secure Shell 用户的标识和密码对他们进行认证。建立加密通道后将发送密码和用户标识。用户标识和密码对可以是存储在本地的 12 对用户标识和密码中的一对或是存储在 LDAP 服务器上的用户标识和密码对。不支持公用密钥认证。

生成 **Secure Shell** 服务器密钥

使用 Secure Shell 服务器密钥向客户机认证 Secure Shell 服务器的身份。在创建新的 Secure Shell 服务器专用密钥之前必须禁用 Secure Shell。在启用 Secure Shell 服务器之前，您必须创建服务器密钥。

当您请求新的服务器密钥时，将创建 Rivest、Shamir 和 Adelman（RSA）密钥和 DSA 密钥以允许您从 SSH V1.5 或 SSH V2 客户机访问管理模块。为实现安全性，在配置的保存和恢复操作中不会备份 Secure Shell 服务器专用密钥。

提供以下 SSH 客户机。尽管已测试一些 SSH 客户机，但不会明确指出是否支持特定 SSH 客户机。

- 随 Linux、AIX® 和 UNIX® 等操作系统分发的 SSH 客户机（有关信息，请参阅您的操作系统文档）。Red Hat Linux 7.3 的 SSH 客户机曾用于测试命令行界面。
- cygwin 的 SSH 客户机（有关信息，请访问 http://www.cygwin.com）。

下表显示了 SSH V1.5 和 V2.0 支持的加密算法的类型。

算法	**SSH V1.5** 客户机	**SSH V2.0** 客户机
公用密钥交换	SSH 1 密钥交换算法	Diffie-Hellman-group 1-sha-1
主机密钥类型	RSA（1024 位）	DSA（1024 位）
批量密码算法	3-des	3-des-cbc 或 blowfish-cbc
MAC 算法	32 位 crc	Hmac-sha1

完成以下步骤以创建新的 Secure Shell 服务器密钥：

1. 在导航窗格中，单击 **MM** 控制 → 安全性。
2. 滚动到 **Secure Shell**（**SSH**）服务器部分并确保已禁用 Secure Shell 服务器。如果尚未禁用它，请选择 **SSH** 服务器字段中的禁用，然后单击保存。
3. 滚动到“SSH 服务器密钥管理”部分。将显示一个类似于下图的页面。



4. 单击生成 **SSH** 服务器专用密钥。将显示一个进度页面。等待操作完成。此步骤可能需要几分钟的时间才能完成。

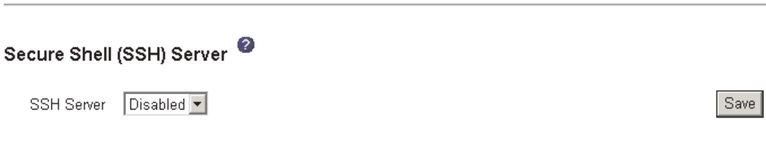
启用 Secure Shell 服务器

您可以从“安全性”页面中启用或禁用 Secure Shell 服务器。您所做的选择只有在重新启动管理模块后才会生效。屏幕上显示的值（启用或禁用）是上一次选择的值，也是管理模块重新启动时使用的值。

注：只有在安装了有效的 Secure Shell 服务器专用密钥时，您才能启用 Secure Shell 服务器。

完成以下步骤以启用 Secure Shell 服务器：

1. 在导航窗格中，单击安全性。
2. 滚动到 **Secure Shell**（**SSH**）服务器部分。将显示一个类似于下图的页面。



3. 单击 **SSH** 服务器字段中的启用。

4. 在导航窗格中，单击重新启动 **ASM** 以重新启动管理模块。

使用 **Secure Shell** 客户机

如果您要使用 Red Hat Linux V7.3 附带的 Secure Shell 客户机，请输入类似于以下示例的命令以启动到网络地址为 192.168.70.2 的管理模块的 Secure Shell 会话：

```
ssh -x -l USERID 192.168.70.2
```

其中 -x 表明不使用 X Window System 转发，而 -l 表明会话将使用用户标识 USERID。

配置 **Wake on LAN**

完成以下步骤以配置 BladeCenter T 单元中的 Wake on LAN 功能：

1. 请记录每台刀片服务器中的集成以太网控制器的 MAC 地址。您可以使用每台刀片服务器的配置／设置实用程序（设备和 **I/O** 端口 → 系统 **MAC** 地址）或查看每台刀片服务器机箱底部的条形码标签找到此信息。每台刀片服务器可能还有一个印有 MAC 地址的活动标签。配置远程系统使用 Wake on LAN 功能启动刀片服务器时需要这些 MAC 地址：远程系统通过将 Wake on LAN 命令（魔术包帧）发送到 MAC 地址来发出它。
2. 确保已启用 BladeCenter T 管理模块中的 Wake on LAN 功能（管理模块 Web 界面中的刀片任务 → 电源／重新启动和刀片任务 → 配置）。
3. 确保已启用 I/O 模块托架 1 和 2 中以太网交换机模块或 pass-thru 模块的外部端口（管理模块 Web 界面中的 **I/O** 任务 → 管理 → 高级管理）。如果未启用外部端口，BladeCenter T 单元中的刀片服务器将无法与外部网络进行通信。

验证 **Wake on LAN** 配置

完成以下步骤以验证 Wake on LAN 功能是否已正确配置并工作正常：

1. 启动刀片服务器操作系统。
2. 尝试 ping 发出 Wake on LAN 命令的远程计算机（魔术包帧）。成功的 ping 操作可以验证网络的连接状况。
3. 确保刀片服务器是键盘、视频和鼠标（KVM）的当前所有者。
4. 关闭刀片服务器，在通过 USB 连接的软盘驱动器中插入一张 DOS 启动软盘，然后重新启动刀片服务器。
5. 当出现 A:\ 提示符时，使用电源控制按键关闭刀片服务器。
6. 从远程计算机发出 Wake on LAN 命令（魔术包帧）。

   如果 Wake on LAN 功能配置正确并且工作正常，将唤醒一台刀片服务器。这是使用操作系统确定某台刀片服务器或 BladeCenter T 配置问题或设备驱动程序问题的一种好方法。

特定于 **Linux** 的配置

为 Red Hat 或 SUSE LINUX 配置 Wake on LAN 功能时，请完成以下步骤：

1. 输入以下命令：

   ```
   insmod bcm5700.o enable_wol=1,1
   ```

开关 `enable_wol=1,1` 参数告诉设备驱动程序为一台刀片上的两个 Broadcom 控制器启用 Wake on LAN 功能。因为有两个 Broadcom 控制器，所以您必须为它们各发出一个 1。

2. 为您的 Linux 映像重新编译设备驱动程序。例如，在 Red Hat Linux 中编译的设备驱动程序不一定能在 SUSE LINUX 中正常使用。有关编译设备驱动程序的信息，请参阅您的操作系统随附的文档。

   要在 Red Hat Linux 中成功编译 Broadcom 设备驱动程序，缺省安装还不足够，因为它未包含成功编译所需的所有文件。选择软件和内核开发软件包的 Red Hat Linux 定制安装包含成功编译设备驱动程序所需的文件。

使用配置文件

在管理模块 Web 界面中，单击 **MM** 控制 → 配置文件来备份和恢复管理模块配置。

Backup MM Configuration

To backup the configuration, click "Backup." You can view the current configuration summary before backing it up.

Backup

Restore MM Configuration

To restore the MM configuration, select a file and click "Restore." To modify the configuration and then restore it, select a file and click "Modify & Restore."

Select configuration file to restore

Browse...

Restore Modify and Restore

注：如果您无法通过 Web 界面与替换管理模块进行通信，该 IP 地址与卸下的管理模块的 IP 地址可能不同。按下 IP 复位按钮将管理模块重置为出厂时的缺省 IP 地址；然后使用出厂时的 IP 地址（有关出厂时的 IP 地址，请参阅第 13 页的『配置管理模块进行远程访问』）访问管理模块并配置管理模块或装入已保存的配置文件。

备份当前的配置

您可以将当前管理模块配置的副本下载到运行管理模块 Web 界面的客户机计算机上。如果意外地更改或损坏了管理模块配置，您可以使用该备份副本来恢复管理模块配置。将它作为一个基础模板，您可以修改它来配置多个具有相似配置的管理模块。

完成以下步骤以备份当前配置：

1. 登录到您要备份其当前配置的管理模块。有关更多信息，请参阅第 16 页的『启动管理模块 Web 界面』。
2. 在导航窗格中，单击 **MM** 控制 → 配置文件。
3. 在备份 **MM** 配置部分中，单击查看当前配置摘要。

   注：不会备份“安全性”页面中的安全性设置。
4. 验证设置，然后单击关闭。

5. 要备份配置，单击备份。
6. 输入备份名称，选择保存文件的位置，然后单击保存。
   - 在 Netscape Navigator 中，单击保存文件。
   - 在 Microsoft Internet Explorer 中，选择将该文件保存到磁盘，然后单击确定。

恢复和修改 **ASM** 配置

您可以完整恢复已保存的配置，也可以在将配置恢复到管理模块之前修改已保存的配置中的关键字段。在恢复前修改配置文件可以帮助您设置多个具有相似配置的管理模块。您可以快速指定需要唯一值的参数（如名称和 IP 地址）而不必输入常见的共享信息。

完成以下步骤以恢复或修改当前配置：

1. 登录到您要恢复配置的管理模块。有关更多信息，请参阅第 16 页的『启动管理模块 Web 界面』。
2. 在导航窗格中，单击 **MM** 控制 → 配置文件。
3. 在恢复 **MM** 配置部分中，单击浏览。
4. 单击所需的配置文件，然后单击打开。文件（包括完整路径）将出现在浏览旁的框中。
5. 如果您不想更改配置文件，单击恢复。将打开一个新的窗口，其中显示管理模块配置信息。验证这是您要恢复的配置。如果配置不正确，请单击取消。

   如果要在恢复之前更改配置文件，单击修改并恢复以打开一个可编辑的配置摘要窗口。初始情况下，将只显示可以更改的字段。要在该视图和完整配置摘要视图之间切换，单击窗口顶部或底部的切换视图按钮。

   注：当您单击恢复或修改并恢复时，如果您尝试恢复的配置文件是由一个固件版本较早的管理模块创建的（因此功能较少），则可能打开一个警报窗口。该警报消息包含一系列完成恢复后您必须配置的系统管理功能。一些功能需要在多个窗口中进行配置。
6. 要继续将该文件恢复到管理模块，单击恢复配置。更新管理模块上的固件时，将显示一个进度指示器。将打开一个确认窗口以验证更新是否成功。

   注：恢复操作不会恢复“安全性”页面中的安全性设置。要修改安全性设置，请参阅第 47 页的『安全 Web 服务器和安全 LDAP』。
7. 接收到恢复过程已完成的确认后，在导航窗格中单击 **MM** 控制 → 重新启动 **MM**；然后单击重新启动。
8. 单击确定以确认您要重新启动管理模块。
9. 单击确定以关闭浏览器窗口。
10. 要再次登录到管理模块中，请启动浏览器并按登录过程操作。

使用远程磁盘功能

您可以从“远程控制”窗口（请参阅第 25 页的『远程控制』）将远程客户机上的 CD-ROM 驱动器或软盘驱动器指定或安装到刀片服务器上。您也可以使用该窗口指定远程客户机上的磁盘映像或 CD 映像供刀片服务器使用。

您可以使用远程磁盘来实现各种功能，例如：重新启动刀片服务器、更新固件、在刀片服务器上安装新的软件以及在刀片服务器上安装或更新操作系统。指定远程磁盘后，使用远程控制台功能来访问它。远程磁盘在刀片服务器上显示为 USB 驱动器。

您的操作系统必须提供 USB 支持才能使用远程磁盘功能。以下操作系统提供 USB 支持：

- Microsoft Windows Server 2003
- Microsoft Windows 2000 （带 Service Pack 4 或后续版本）
- Red Hat Linux V7.3
- SUSE LINUX V8.0

此外，客户机（远程）系统必须安装 Microsoft Windows 2000 或后续版本以及 Java 1.4 或后续版本插件。客户机系统还必须配备 700 MHz 或更高速度的 Intel™ Pentium® III 或后续版本的微处理器（或等效的微处理器）。

完成以下步骤将远程客户机上的磁盘驱动器或磁盘映像安装到刀片服务器上：

1. 启动管理模块 Web 界面（请参阅第 16 页的『启动管理模块 Web 界面』）。
2. 在导航窗格中，单击刀片任务 → 远程控制。
3. 在启动远程控制部分中，单击启动远程控制。
4. 在远程磁盘部分中，选择相应的硬盘驱动器或映像以便从远程磁盘驱动器选择器左侧选择安装它们；然后单击 **>>** 确定选择内容并将它们移动到远程磁盘驱动器选择器的右侧。要取消选择多个项，在远程磁盘驱动器选择器的右侧选择它们，然后单击 **<<**。

   当选择一个软盘驱动器或映像文件并将它移动到驱动器选择器的右侧时，您可以选择将磁盘映像保存在管理模块的随机存取存储器（RAM）中。这使得磁盘映像能始终安装在刀片服务器上，以便您以后访问磁盘映像（即使已终止 Web 界面会话）。当关闭远程控制窗口时，将卸下未保存到管理模块的已安装的驱动器。

   管理模块上最多可以存储一个软盘驱动器或驱动器映像。驱动器或映像内容的大小必须小于等于 1.44 MB。

   要点：重新启动管理模块或更新管理模块固件时，磁盘映像将丢失。要使用安装的磁盘，请使用“远程控制台”功能。安装的磁盘将显示为连接到服务器的 USB 磁盘驱动器。
5. 单击写保护以防止向安装的驱动器写入数据。
6. 在远程磁盘驱动器选择器的右侧，选择要安装的一个或多个驱动器或映像；然后单击安装驱动器。

   安装的驱动器或磁盘映像将作为连接到刀片服务器的 USB 设备。要刷新远程客户机上的可用驱动器列表，单击刷新列表。

使用完驱动器或磁盘映像后，完成以下步骤以关闭并卸下它：

1. 完成您的操作系统关闭并卸下远程磁盘或映像所需的任何过程。有关信息和说明，请参阅您的操作系统的文档。

   对于 Microsoft Windows 操作系统，完成以下一种过程以关闭并卸下驱动器或驱动器映像：
   - 如果 Windows 任务栏中显示一个拔出或弹出硬件图标，完成以下步骤：
     a. 双击拔出或弹出硬件图标。
     b. 选择 **USB Mass Storage Device** 并单击停止。
     c. 单击关闭。
   - 如果 Windows 任务栏中没有拔出或弹出硬件图标，完成以下步骤：
     a. 在 Microsoft Windows 控制面板中，双击添加/删除硬件；然后单击下一步。
     b. 选择卸载/拔掉设备；然后单击下一步。
     c. 单击拔出/弹出设备；然后单击下一步。
2. 在管理模块 Web 界面的“远程控制”窗口的远程磁盘部分中，单击卸下驱动器。

附录 A. 获取帮助和技术协助

如果您需要帮助、服务或技术协助，或者只希望了解有关 IBM 产品的更多信息，则可从 IBM 找到各种可用的资源来帮助您。本附录中的信息包括：到何处寻找有关 IBM 及 IBM 产品的更多信息、如果 xSeries®、BladeCenter 或 IntelliStation® 系统有问题该采取什么措施以及如果有必要该向谁请求服务。

在打电话请求服务之前

在您请求服务之前，确保已采取以下步骤来尝试自行解决问题：

- 检查所有电缆以确保它们都已连接。
- 检查电源开关以确保系统已开启。
- 使用系统文档中的故障诊断信息，并使用系统随附的诊断工具。IBM *xSeries 文档* CD 中的*《硬件维护手册和故障诊断指南》*或 IBM Support Web 站点上的 IntelliStation *《硬件维护手册》*包含了有关诊断工具的信息。
- 转至位于 http://www.ibm.com/pc/support/ 的 IBM Support Web 站点，查看技术信息、提示、技巧以及新的设备驱动程序或提交获取信息的请求。

按照 IBM 在联机帮助或随您的系统和软件附带的出版物中提供的故障诊断过程，您能够解决许多问题而无需外界帮助。随您的系统一起提供的信息也描述了您能够执行的诊断测试。大多数 xSeries 和 IntelliStation 系统、操作系统以及程序都附带包含了诊断过程和错误消息以及错误代码的说明信息。如果您怀疑软件有问题，请参阅有关操作系统或程序的信息。

使用文档

如果有关于您的 IBM xSeries 或 IntelliStation 系统以及预安装软件的信息，您可以从系统随附的文档中获得它们。该文档包含印刷书籍、联机丛书、自述文件和帮助文件。有关使用诊断程序的说明，请参阅系统文档中的故障诊断信息。故障诊断信息或诊断程序可能会告诉您需要其它的或更新的设备驱动程序或其它软件。您可以从万维网上 IBM 维护的页面获取最新的技术信息并下载设备驱动程序和更新。要访问这些页面，请转至 http://www.ibm.com/pc/support/ 并按照说明进行操作。另外，您还可以通过 IBM Publications Ordering System 订购出版物，该系统的地址是 http://www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi。

从万维网获取帮助和信息

在万维网上，IBM Web 站点提供有关 IBM xSeries 和 IntelliStation 产品、服务和支持的最新信息。IBM xSeries 信息的地址是 http://www.ibm.com/eserver/xseries/。IBM IntelliStation 信息的地址是 http://www.ibm.com/pc/intellistation/。

您可以在 http://www.ibm.com/pc/support/ 找到有关您的 IBM 产品（包括支持的选件）的服务信息。

软件服务和支持

通过 IBM Support Line，您可以付费获得电话帮助，帮助内容涉及 xSeries 服务器、IntelliStation 工作站和设备的使用、配置和软件问题。要了解在您所在的国家或地区 Support Line 支持哪些产品，请转至 http://www.ibm.com/services/sl/products/。

有关 Support Line 和其它 IBM 服务的更多信息，请转至 http://www.ibm.com/services/，或转至 http://www.ibm.com/planetwide/ 查询支持电话号码。在美国和加拿大，请致电 1-800-IBM-SERV（1-800-426-7378）。

硬件服务和支持

您可以通过 IBM Services 获得硬件服务，或者如果您的经销商由 IBM 授权提供保修服务的话，您也可以通过 IBM 经销商获得硬件服务。请转至 http://www.ibm.com/planetwide/ 查询支持电话号码，或（在美国和加拿大）致电 1-800-IBM-SERV（1-800-426-7378）。

在美国和加拿大，每天 24 小时，每周 7 天都可获得硬件服务和支持。在英国，周一至周五的上午九点至下午六点可获取这些服务。

附录 B. 声明

本信息是为在美国提供的产品和服务编写的。

IBM 可能在其他国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您当前所在区域的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务，则由用户自行负责。

IBM 公司可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并未授予用户使用这些专利的任何许可。您可以用书面方式将许可查询寄往：

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

International Business Machines Corporation“按现状”提供本出版物，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、适销和适用于某种特定用途的保证。某些国家或地区在某些交易中不允许免除明示或暗含的保证。因此本条款可能不适用于您。

本信息中可能包含技术方面不够准确的地方或印刷错误。此处的信息将定期更改；这些更改将编入本出版物的新版本中。IBM 可以随时对本资料中描述的产品和／或程序进行改进和／或更改，而不另行通知。

本信息中对非 IBM Web 站点的任何引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。那些 Web 站点中的资料不是 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

版本声明

商标

下列术语是 International Business Machines Corporation 在美国和／或其他国家或地区的商标：

Active Memory	Predictive Failure Analysis
Active PCI	PS/2

Active PCI-X
Alert on LAN
BladeCenter
C2T Interconnect
Chipkill
EtherJet
e-business 徽标
@server
FlashCopy
IBM
IBM（徽标）
IntelliStation
NetBAY
Netfinity
NetView
OS/2 WARP
ServeRAID
ServerGuide
ServerProven
TechConnect
ThinkPad
Tivoli
Tivoli Enterprise
Update Connector
Wake on LAN
XA-32
XA-64
X-Architecture
XceL4
XpandOnDemand
xSeries

Intel、MMX 和 Pentium 是 Intel Corporation 在美国和／或其他国家或地区的商标。

Microsoft、Windows 和 Windows NT 是 Microsoft Corporation 在美国和／或其他国家或地区的商标。

UNIX 是 The Open Group 在美国和其他国家或地区的注册商标。

Java 和所有基于 Java 的商标和徽标是 Sun Microsystems, Inc. 在美国和／或其他国家或地区的商标或注册商标。

Adaptec 和 HostRAID 是 Adaptec, Inc. 在美国和／或其他国家或地区的商标。

Red Hat、Red Hat“Shadow Man”徽标和所有基于 Red Hat 的商标和徽标是 Red Hat, Inc. 在美国和／或其他国家或地区的商标或注册商标。

其他公司、产品或服务名称可能是其他公司的商标或服务标记。

重要注意事项

处理器速度表示微处理器的内部时钟速度；其它因素也会影响应用程序性能。

CD-ROM 驱动器速度列出了可变的读取速率。实际速度会发生变化，并且经常会小于可能达到的最大速度。

当指处理器存储量、实际和虚拟存储量或通道量时，KB 代表大约 1,000 字节，MB 代表大约 1,000,000 字节而 GB 代表大约 1,000,000,000 字节。

当指硬盘驱动器容量或通信量时，MB 代表 1,000,000 字节而 GB 代表 1,000,000,000 字节。用户可用的总容量可能因操作环境不同而异。

内置硬盘驱动器的最大容量是指用 IBM 提供的当前受支持的最大容量的驱动器来替换任何标准硬盘驱动器，并装满所有硬盘驱动器托架时的容量。

最大内存可能需要把标准内存更换为可选内存条。

IBM 对 ServerProven® 的非 IBM 的产品和服务不作任何陈述或保证，包括但不限于对适销和适用于某种特定用途的暗含保证。这些产品由第三方单独提供和保证。

IBM 对于非 IBM 产品不作任何陈述或保证。对于非 IBM 产品的支持（如果存在）由第三方而非 IBM 提供。

某些软件可能与其零售版本（如果可用）不同，并且可能不包含用户手册或所有程序功能。

产品回收和处理

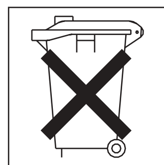
此单元包含各种材料，如电路板、电缆、电磁兼容性垫圈和接口，它们可能包含铅和铜铍合金，在产品使用期结束后需要进行特殊的操作和处理。处理此单元之前，必须根据适用的法规卸下并且回收或废弃这些材料。IBM 在一些国家或地区提供产品回收计划。可以在 IBM 的因特网站点 http://www.ibm.com/ibm/environment/products/prp.shtml 中找到提供的有关产品回收的信息。

电池回收计划

本产品可能包含密封的铅酸、镍镉、镍氢、锂或锂离子电池。有关特定的电池信息，请查阅用户手册或服务手册。必须正确回收或处理电池。您所在的地区可能没有回收设施。有关在美国以外的地区处理电池的信息，请转至 http://www.ibm.com/ibm/environment/products/batteryrecycle.shtml 或与当地的废品处理机构联系。

在美国，IBM 建立了用于重复使用、回收或正确处理来自 IBM 设备的使用过的 IBM 密封铅酸、镍镉、镍氢和电池组的收集过程。有关正确处理这些电池的信息，请拨打 1-800-426-4333 联系 IBM。拨打电话前，请查看电池上列出的 IBM 部件号。

在荷兰，以下内容适用。



电子辐射声明

联邦通信委员会（FCC）声明

注：依据 FCC 规则的第 15 部分，本设备经过测试，符合 A 类数字设备的限制。设计这些限制的目的是当设备运行在商业环境中时，可针对有害干扰提供合理的保护。此设备生成、使用并可辐射射频能量，并且如果不按照说明手册进行安装和使用，可能会对无线电通信产生有害干扰。在居民区运行此设备很可能产生有害干扰，在这种情况下将由用户自行承担清除干扰的费用。

必须使用正确屏蔽并接地的电缆和接口，以满足 FCC 辐射限制。因使用非推荐的电缆和接口，或者对此设备进行未经授权的更改或修改而导致的任何射频或电视干扰，IBM 概不负责。未经授权的更改或修改可能会使用户操作该设备的权限失效。

该设备符合 FCC 规则第 15 部分的规定。操作该设备应符合以下两个条件：（1）此设备应不会导致有害干扰，并且（2）此设备必须能接受接收到的任何干扰，包括可能导致非期望操作的干扰。

加拿大工业部 A 类辐射一致性声明

此 A 类数字设备符合加拿大 ICES-003 标准。

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

澳大利亚和新西兰 A 类声明

警告： 本产品为 A 类产品。在家用环境中，本产品可能引起射频干扰，此时用户可能需要采取适当的措施。

英国远程通信安全要求

对客户的声明

此设备在英国得到间接连接至公共电信系统的批准，批准号为 NS/G/1234/J/100003。

欧盟 EMC 指令一致性声明

依据各成员国有关电磁兼容性的相近法律，本产品符合欧盟委员会指令 89/336/EEC 中的保护要求。IBM 对任何因擅自改动本产品（包括安装非 IBM 选件卡）而导致的不满足保护要求的任何故障概不负责。

本产品经过测试并且符合根据 CISPR 22/European Standard EN 55022 的 A 类信息技术设备的限制。A 类设备限制源自于商业和工业环境以对许可通信设备的干扰提供合理的保护。

警告： 本产品为 A 类产品。在家用环境中，本产品可能引起射频干扰，此时用户可能需要采取适当的措施。

台湾语 A 类警告声明

警告使用者:
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

中文 A 类警告声明

声　明
此为 A 级产品。在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

日本干扰自愿控制委员会（VCCI）声明

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

索引

[A]

安全性 37，38
安全性，配置 48
安全 Web 服务器和安全 LDAP
  概述 47
  配置安全性 48
  为安全 Web 服务器启用 SSL 55
  为 LDAP 客户机启用 SSL 57
  SSL 服务器证书管理 49
  SSL 客户机受信任的证书管理 55
  SSL 客户机证书管理 55
  SSL 证书概述 48
安装远程驱动器或映像 61

[B]

帮助 18
保存配置文件 60

[C]

错误日志
  请参阅 事件日志

[D]

刀片服务器
  固件更新 27
电源指示灯
  管理模块 3
  KVM 模块 6
电子辐射 A 类声明 69
端口 34
  请参阅 接口
端口指定 34

[G]

固件更新
  刀片服务器 27
  管理模块 39
  I/O 模块 31
管理模块
  固件更新 39
  冗余
    手动交接 40
  指示灯 3
    错误 3

管理模块 *(续)*
  指示灯 *(续)*
    电源 3
    活动 3
  IP 复位按钮 3
管理模块 Web 界面
  启动 16

[H]

恢复配置文件 60

[J]

加密算法 58
键盘接口 4
接口
  键盘 4
  视频 5
  输入／输出 6
  以太网 6
  远程管理 6
  远程管理和控制台 6
  KVM 模块 4
  PS/2 鼠标 5
  telco 警报 6
警报中的事件日志 34

[L]

联机文档 2
连线，远程连接以太网端口 11

[M]

美国电子辐射 A 类声明 69
美国 FCC A 类声明 69

[P]

配置
  DNS 42
  LDAP 42
  LDAP 客户机认证 44
  LDAP 搜索属性 45
  Secure Shell 服务器 57
  SMTP 42
  SNMP 40
  Wake on LAN 59

配置 *(续)*
  Wake on LAN（Linux） 59
配置文件
  保存 60
  恢复 60
配置／设置实用程序 15

[Q]

权限，用户 15

[R]

认证，LDAP 32

[S]

商标 67
设置 LDAP 客户机 43
实用程序，配置／设置 15
使用权限 15
事件日志 21
事件日志，查看 21
视频接口 5
鼠标接口 5
算法，加密 58

[T]

替换模块，无法通信 60

[W]

网络
  连接 11
网络协议
  配置 DNS 42
  配置 LDAP 42
  配置 SMTP 42
  配置 SNMP 40
  配置 SSL 47
无法与替换模块进行通信 60

[X]

协议
  DNS 42
  SMTP 42
  SNMP 40
  SSL 47

[Y]

以太网
  端口，连线 11
  活动指示灯 12
  接口 6
  链路状态指示灯 12
  配置远程连接 13
  以太网活动指示灯 6
  以太网接口、远程管理和控制台 6
  以太网链路状态指示灯 6
远程磁盘 26，61
远程管理接口 6
远程控制 26
远程控制台 26
远程连接 11

[Z]

指示灯
  管理模块 3
    错误 3
    电源 3
    活动 3
  警报 4
    次要 4
    严重 4
    主要 4
  设置颜色 21
  系统状态面板
    电源 4
    位置 4
  以太网活动 6，12
  以太网链路状态 6，12
  KVM 模块 4
    系统状态面板 4
  LAN 模块 6
    电源 6
    以太网活动 6
注意事项
  电子辐射 69
  FCC，A 类 69
注意事项，重要 68

A

A 类电子辐射声明 69

B

BladeCenter T 单元
  配置 9

D

DNS 37
DNS，配置 42

F

FCC A 类声明 69

I

IP 复位按钮 60
IP 复位按钮，管理模块 3
I/O 模块
  固件更新 31

K

KVM 模块
  接口
    键盘 4
    视频 4
    鼠标 4
  指示灯
    次要 telco 警报 4
    电源 4
    位置 4
    严重 telco 警报 4
    主要 telco 警报 4

L

LAN 模块
  功能 6
  指示灯
    以太网活动 6
    以太网链路 6
LDAP 37
  概述 42
  配置客户机认证 44
  配置搜索属性 45
  设置客户机 43
LDAP 认证 32

S

Secure Shell 服务器
  概述 57
  启用 58
  生成专用密钥 57
Secure Shell 连接客户机 58
serial over LAN 29
SMTP 37
SMTP，配置 42
SNMP 37
SNMP，配置 40
SOL 29
SSH 38
SSH 客户机 58
SSL 安全协议 47
SSL 服务器证书管理 49
SSL 客户机受信任的证书管理 55
SSL 客户机证书管理 55
SSL 证书概述 48
SSL，启用
  为安全 Web 服务器 55
  为 LDAP 客户机 57
SSL，LDAP 38

T

TCP 日志 37
TCP 日志，查看 37
telco 警报接口 6

W

Wake on LAN
  配置 59
  验证配置 59
  Linux 配置 59
Web 浏览器，受支持的 9



部件号： 11R2160

中国印刷

(1P) P/N: 11R2160

